

Seguridad en Redes

Alejandro Corletti Estrada

www.darFe.es

Seguridad en Redes

Madrid, octubre de 2016

RPI (Madrid): M-6249/2016

ISBN: 978-84-617-5291-1



Alejandro Corletti Estrada

(acorletti@DarFe.es - acorletti@hotmail.com)

www.darFe.es

Este libro en formato electrónico con extensión "**PDF**" es el que se encuentra disponible gratuitamente en Internet.

La versión impresa del mismo (*que sí es de pago*) puede ser solicitada por correo electrónico a la cuenta:

info@darFe.es

Agradecimientos

A todos los que a través del apoyo, reconocimiento y agradecimientos de la obra anterior "**Seguridad por Niveles**", me han dado ánimo para seguir reuniendo temas y escribir este nuevo libro.

A mi "gran Maestro" **Antonio Castro Lechtaler**, con el que tuve el placer de iniciarme en la docencia y compartir hermosos años dentro de su Cátedra.

A **Chema Alonso** que con infinita paciencia supo dedicarme algo de su escaso tiempo para escribir uno de los prólogos de este libro.

A "*Nacho*" (**José Ignacio Bravo Vicente**) y "*Paco*" (**Francisco Martín Vázquez**), quienes con su *buena onda* y enorme conocimiento, logran día a día mantenerme en este ritmo del "cacharreo", bajándome de las nubes de la teoría de Seguridad y Redes.

A un sinnúmero de **Operadores** de red, gente de **Seguridad** y de **Auditoría** de muchos Países (*cada uno de ellos sabe bien a quiénes me refiero*), que vienen sufriéndome y aguantando desde hace varios años (*muchas gracias, de verdad*).

Por qué no también, mi más sincero reconocimiento al "**Grupo Telefónica**" que por más de veinte años me permitió jugar en esta "Primera División" aprendiendo, entendiendo y coordinando redes con los mejores profesionales y equipos (de avanzada y última generación) de la Liga Internacional (o mercado).

Por último también….. gracias a todas las revistas, editoriales y medios de difusión que por "no encajar" en sus sistemas comerciales, no tuvieron mucha intención de fomentar este libro, el anterior y en general, ningún tipo de material "Open Source" o de libre difusión. Les agradezco de verdad, pues me han abierto puertas a través de las decenas de miles de lectores, a los que no hubiese podido llegar de su mano. (*tarde o temprano deberán enrolarse en estas nuevas líneas de difusión*).

INDICE



Prólogo 1: Antonio Castro Lechtaler

Cuando el Doctor Ingeniero Alejandro Corletti Estrada me pidió que prologara su libro ***Seguridad en Redes*** vinieron a mi memoria recuerdos muy agradables de muchos años en los que hemos compartido experiencias que se inician a mediados de la década de los años 90 cuando él cursaba la carrera de Ingeniería y empezábamos a hablar de estos temas que hoy nos ocupan a ambos.

Seguridad en Redes es una obra que viene a llenar el amplio vacío existente de libros técnicos de nivel universitario orientados al tema de redes, telecomunicaciones y seguridad, provenientes de escritores hispanohablantes, integrándose así al grupo reducido de autores que hemos tratado de cubrir con este tipo de trabajos las currículas de las materias que se cursan en las Universidades de España y América Latina.

Es conocido el desinterés editorial en este tipo de obras técnicas escritas en idioma español, básicamente a causa de la costumbre de la fotocopia de libros técnicos editados en nuestro idioma, que desconoce el costo que este tipo de publicaciones implica, en una falta de respeto evidente por la propiedad intelectual de los autores latinos así como de la comunidad que los agrupa.

Seguridad en redes es un libro que cuenta con un capitulo introductorio en el que actualiza conocimientos sobre las tecnologías de las redes actuales, tanto fijas como móviles. En esta primera parte clarifica conceptos esenciales sobre conmutación y enrutamiento, los que resultan imprescindibles para entender los aspectos que hacen a la seguridad sobre redes.

El centro de gravedad del desarrollo de la obra está puesto en todos los aspectos que hacen a la seguridad de las redes de teleinformática, temática hoy de fundamental importancia a nivel gubernamental, personal, empresarial y educativa.

El autor deja entrever muy claramente sus puntos de vista sobre los distintos estándares, los que desarrolla con simplicidad y gran profundidad al mismo tiempo. Por otra parte los gráficos que describen protocolos y pilas de acciones han sido confeccionados con gran categoría, lo que no es muy común en obras de este tipo.

El desarrollo de las estrategias de seguridad para grandes redes tiene conceptos que solo pueden surgir de aquel que ha trajinado con intensidad los problemas de seguridad que en ellas se pueden generar al tiempo que explica conceptos esenciales que resultan imprescindibles para entender los aspectos que hacen a la seguridad sobre las redes.

En resumen: la obra será una herramienta de consulta y uso permanente para aquellos que transitan por el camino de los diversos aspectos que involucran el tema de seguridad en las redes de comunicaciones.

Sin duda el autor se ha transformado, y esta obra lo pone de manifiesto, en un referente internacional en esta temática, ya que su trabajo en el área de la Seguridad Informática así lo acredita.

Para un profesor siempre es gratificante saber que la siembra ha sido efectuada sobre el surco abierto en tierra tan fértil, y que ésta se ha transformado en una abundante cosecha. En lo personal, me siento orgulloso de haber tenido alumnos como Alejandro, que no solo nos ha igualado sino que con su esfuerzo y capacidad nos han sobrepasado con tanto éxito.

Él es uno de uno de aquellos que percibieron el tañido de las campanas de las tecnologías emergentes y de la nueva sociedad de la información y las comunicaciones que hace no más de veinte años no se veía aun tan clara. Creyó en el nuevo mundo en ciernes y acertó como los visionarios, que normalmente no abundan.

No me queda más que agradecer y felicitar la dedicación, el esfuerzo y también el cariño que el autor ha puesto en la preparación de este libro.

Ciudad de Buenos Aires, primavera del año 2016.

Profesor ANTONIO RICARDO CASTRO LECHTALER

Profesor Titular Consulto

Universidad de Buenos Aires

Universidad de la Defensa



Prólogo 2: Ser un hacker y no un profesional (Por Chema Alonso)

Quiere el destino que escriba este prólogo solo un par de días después de que tuviera lugar el, hasta ahora, ataque de denegación de servicio distribuida más grande que se recuerda. Con una potencia de hasta 1.2 Terabits por segundo la botnet Mirai ha conseguido marcar el récord en tráfico generado para hacer un ataque contra un objetivo concreto.

Corremos tiempos beligerantes en las redes de comunicaciones en los que los cibercriminales han encontrado en ellas un medio para perpetrar sus ataques con cierta percepción de impunidad al ocultarse en la distancia de países remotos con leyes no adaptadas que dejan que se escapen como polvo en los dedos.

Proteger este activo tan preciado que la tecnología nos ha dado es responsabilidad de todos. Desde el dueño de una impresora en su casa hasta el administrador de una pequeña red de equipos en una empresa pasando, lógico está, por los grandes proveedores de servicios en Internet. Cada fallo de seguridad en esta vasta y creciente red de redes puede ser utilizado por un adversario para conseguir una ventaja en un ataque y así, como hemos visto en el ataque que citaba al principio, la botnet Mirai se ha aprovechado de dispositivos como impresoras, routers, switches o cámaras de vigilancia mal configuradas, con bugs conocidos o contraseñas por defecto, para conseguir un número tal de equipos infectados que una empresa como DYN, que da soporte a una parte importante de los servicios DNS de Internet, no pueda contenerla.

Conocer nuestras redes, los rincones más pequeños y escorados de las mismas, para evitar que el eslabón más débil de esta cadena sea un dispositivo que forma parte del Shadow IT o el Shadow IoT de nuestra organización es fundamental. Pero más lo es conocer cómo funcionan y mantener la seguridad del mismo a lo largo del tiempo.

Decía la definición que hace el Internet Engineering Task Force en su RFC 1983 titulado Internet User' Glossary que un Hacker es:

> *A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term.*

Y es así lo que necesitamos todos que seas en tu red. Un auténtico hacker que tenga un conocimiento íntimo de cómo funciona tu red. Cuáles son los protocolos que están circulando por ellas, cómo están configurados, cómo se pueden mejorar y cuáles son los rastros que deben levantar una alerta en tus mecanismos de detección para saber que algo está pasando por ellas que no debiera.

Debes conocer todo lo que puedas tu red de comunicaciones. Saber cómo siente, piensa y respira cada poro de ella. Cada router, cada switch, cada firewall, cada equipo

que envía o recibe tráfico por el medio que sea, por el protocolo que sea, por la aplicación que sea. Es tu red y debes conocerla como si la hubieras construido tú, debes ser el hacker de tu red y aprender de ella día a día.

En mi vida profesional, ya más larga de lo que me gustaría para poder disfrutar más de los muchos momentos que me toquen por venir aún, me he topado con una gran cantidad de informáticos que realmente no adoraban esta profesión. Profesionales que lo eran porque trabajaban de esto, pero que por falta de pasión y dedicación a conocer lo que tenían entre manos no deberían tener ese título.

Los que de verdad amamos este trabajo no escatimamos esfuerzos en aprender más día a día de lo que tenemos entre manos, en conocer aquello que desconocemos, en disfrutar del trabajo que nos llevó a meternos en esta afición que se convirtió en profesión.

Llegados a este punto debes hacerte a ti mismo esta pregunta. Debes preguntarte qué tipo de profesional quieres ser. Uno de esos que lo es por la tarjeta y la posición laboral o uno de esos que aprende todo lo que puede porque es un hacker que adora la tecnología. Decide tú. Tú manejas tu tiempo, tu vida, tus esfuerzos y tu carrera profesional. Hoy, y ahora, es el momento de que aprendas un poco más para que mañana puedas aprender un poco más sobre lo ya aprendido. Sé un hacker y no un trabajador de la informática.

Aprende todo lo que puedas y haz que tu trabajo sea tu pasión y que tu pasión sea tu trabajo. Solo así podrás ocuparte correctamente de la seguridad de tus redes.

Chema Alonso
chema@11paths.com
http://twitter.com/chemaalonso
http://www.elevenpaths.com

Prólogo del autor

La idea de escribir este segundo libro como continuación de "**Seguridad por Niveles**" fue nuevamente intentar reagrupar y reunir en un solo texto la cantidad de apuntes, cursos y artículos que tenía dando vueltas por Internet, esta vez con la experiencia de haber lanzado una edición previa y con el claro horizonte de lo que representa ofrecer para su libre distribución tantos años de esfuerzo…… con sus enormes satisfacciones, pero también con algún que otro sinsabor que espero esta vez sean mínimos.

Manteniendo mi filosofía "**Open Source**" me propuse difundirlo una vez más de forma gratuita para que pueda aprovecharlo todo aquel que le sea de utilidad en sus estudios, pero reservándome este derecho en el caso comercial.

Como todo desarrollo tecnológico de este siglo, estimo que a medida que pase el tiempo contendrá conceptos o herramientas que van quedando fuera de vigor, de ser así os ruego encarecidamente que me lo hagáis saber a través de mi correo electrónico para poder subsanarlos, también si halláis errores de forma o fondo, los cuales seguramente estarán omnipresentes como en todo escrito.

Este libro siempre estará disponible en la Web: www.darFe.es, seguramente en otros sitios más y lo hallarás fácilmente con cualquier buscador de Internet. También encontraréis muchas prácticas y capturas de tráfico que se pueden descargar de esta misma Web.

Por último os pido que sepáis aceptar que todo esto lo hago con la mejor buena voluntad y dentro de mis limitaciones, así que "no seáis duros con esta obra", es sencillamente una sana y humilde intención de aportar algo en la red, y nada más.

Afectuosamente:

Alejandro Corletti Estrada

acorletti@DarFe.es

acorletti@hotmail.com

1. Historia y evolución de redes

Para comprender la envergadura del problema al que nos enfrentamos, hemos decidido abordarlo a través de la presentación cronológica del diseño que hoy nos permite interconectar al mundo entero para la transmisión de todo tipo de flujos de información.

Si hoy estamos en capacidad de llegar a cualquier lugar se debe a que en sus inicios se sentaron las bases necesarias y, como casi todo en esta vida con sus aciertos y errores se fue avanzando poco a poco hasta llegar al estado actual. La comprensión de hitos importantes de esta evolución es lo que nos permite hacer asociaciones o evaluar el por qué de muchos dispositivos o medidas que se están tomando son necesarias o pueden mejorarse.

1.1. La red de telefonía fija

El comienzo de esta historia está en la red de telefonía fija, y en virtud de su antigüedad es casi una norma en toda operadora de telecomunicaciones la "Omnipresencia" de elementos y ubicaciones de red heredadas que con la evolución vertiginosa actual presentan gran parte de los problemas de seguridad que iremos viendo a lo largo de este texto.

¿Cómo nace esta red?

La red de telefonía conmutada comienza a principios del siglo XX, pueden discutirse las fechas exactas y los países, pero a efectos de este texto consideraremos el despliegue domiciliario a nivel internacional con presencia en gran parte del mundo a mediados de ese siglo. Nace como red analógica únicamente para voz, en la cual se comenzaban a interconectar zonas geográficas de acuerdo a la imagen que se presenta a continuación:

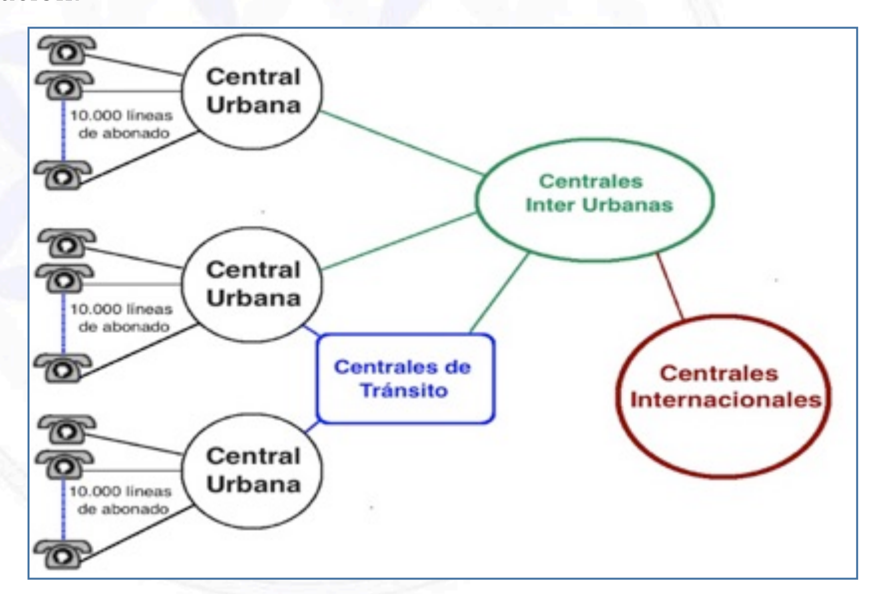


Imagen 1.1 (la red Telefónica Conmutada)

Cada **Central Urbana** (CU) se encontraba lo más próximo al cliente posible, y desde allí nacían 10.000 pares de cobre, de los cuáles la inmensa mayoría aún están en servicio (los últimos 4 dígitos de nuestra líneas actuales de telefonía fija), es el conocido problema actual de la "última milla". Esta CU, se conecta con su correspondiente **Central Interurbana**, la cual como su nombre lo indica interconecta localidades o zonas geográficas, y en la actualidad, por ejemplo en el caso de España se corresponden con los tres primeros dígitos de nuestra telefonía fija. En los casos de localidades de mucha concentración de abonados, aparecen las **Centrales de Tránsito** que sencillamente hacen diferentes tipos de interconexión. Por último esta verdadera "Jerarquía" finaliza con las **Centrales Internacionales**, que son las interconectan diferentes países, en el caso de España a través del prefijo "+34".

Como es natural esta distribución geográfica, implicaba poseer o arrendar locales en diferentes ubicaciones físicas. En muchos casos, es posible jugar más o menos con las distancias, pero el tema de los pares de abonado, no pueden superar los 3 a 4 kilómetros, lo que obliga que las CU, tengan una importante distribución nacional.

Hasta los años 70' toda este red funcionó de esta forma(con sus más y sus menos), pero por estos años aparece la necesidad de interconectar elementos digitales, que sin lugar a dudas lo originan los primeros ordenadores, y lo convierte en imparable la aparición del "PC". Para ello, se debía de alguna forma poder convertir esta señal digital nativa que hablaban estos dispositivos a una señal analógica que era lo que funcionaba en la red, para ello nacen los primeros "modem" (**mo**dulador-**dem**odulador).

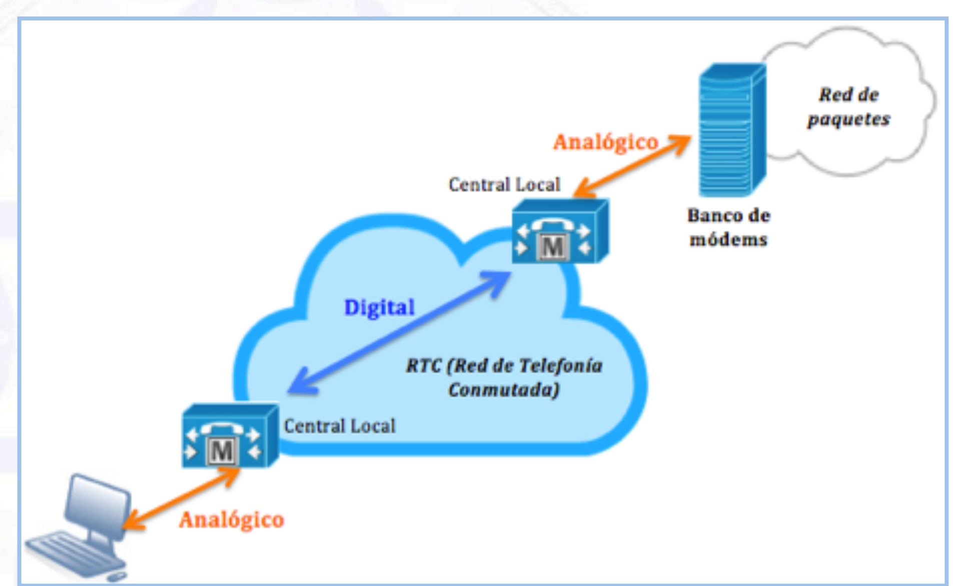


Imagen 1.2 (primeros modem)

Esta generación comienza a poder transmitir en muy baja velocidad, llegando a través de la norma V.34 a unos 34 kbps como máximo y allí alcanza su límite.

En muy poco tiempo comienzan a implantarse en determinados extremos, las primeras redes de conmutación de paquetes (universitarias, investigación, militares), con ello se gana muchísimo en la relación señal ruido y se evita una segunda conversión analógica digital, la norma V.92 fue su máximo exponente superando los 64 kbps.

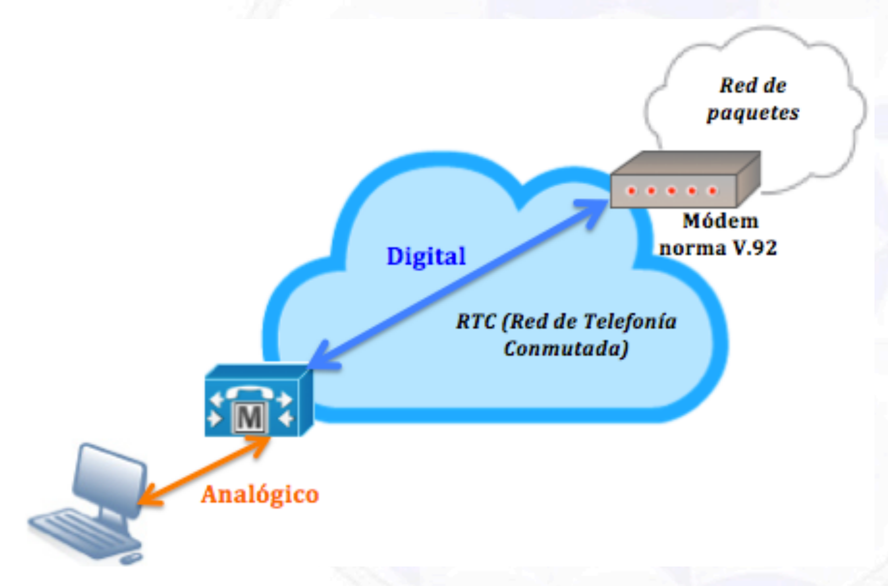


Imagen 1.3 (modem de segunda generación)

El hecho concreto que da inicio a este nuevo cambio, es la implantación de las "Jerarquías digitales", inicialmente Plesiócronas con "PDH" y hoy Sincrónicas con "SDH", a través de estas nuevas tecnologías la voz, cumpliendo con los tres pasos (muestreo, cuantificación y codificación) pasa a transmitirse de forma digital, ocupando canales de 64 Kbps en accesos básicos (BRI = 128 kbps) y primarios (PRI = 2 Mbps con las tramas E1).

Aparece la tecnología **RDSI** (Red Digital de Servicios Integrados) que rápidamente es superada por xDSL (x Digital Subscriber Line), sobre la que nos detendremos aquí.

Estos servicios xDSL se basan sobre todo en nuevas formas de modulación (combinando sobre todo fase y amplitud) a través de "constelaciones" de bits, basados en la capacidad de varias portadoras asociadas a la relación señal ruido de esta "última milla" que hemos mencionado anteriormente; por esta razón es que xDSL es muy dependiente de la distancia y la calidad del par de cobre que llega hasta el domicilio, cuanto mejor sea la relación señal/ruido, mayor cantidad de bits podrá transmitirse por ese par de cobre y por lo tanto mayor ancho de banda se podrá ofrecer. Estas tecnologías xDSL son una familia (HDSL, VDSL, ADSL, etc…), de ellas, la que más empleo se termina haciendo en las redes de Telefonía a nivel domiciliario es ADSL (asynchronous DSL). El concepto de "asíncrono o asimétrico" viene dado en virtud de emplearse dos canales para datos (y un tercero más, independiente para la voz). De los dos canales de datos uno se emplea para "bajada" de información que suele ser de mayor capacidad y otro para "subida" de información que suele ser sensiblemente menor. Las especificaciones técnicas de esta tecnología se encuentran en la

recomendación G.992.1 (G.dmt) y G992.2 (G.lite) de la ITU-T y en el estándar T1.413-1998 de la ANSI. A continuación presentamos una imagen de su funcionamiento:

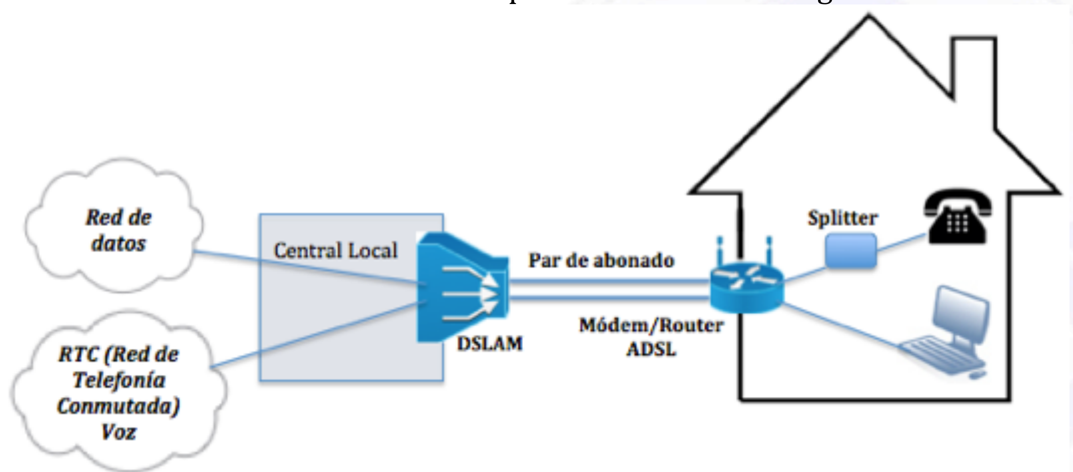


Imagen 1.4 (Arquitectura ADSL)

Como se puede apreciar, se mantiene el mismo para abonado, agregando un modem y un filtro (Splitter) en cada extremo (Dentro del propio DSLAM también se realiza este filtrado), con ello se logra separar la banda baja de esa línea a través de un filtro pasa bajo de 4000 Hz para voz y el resto se deja para datos. Este filtro o splitter es imprescindible para cada teléfono que se coloque en ese hogar, pues sin él sería imposible la comunicación de voz, pues el aparato telefónico estaría recibiendo una gama de frecuencias muy superior a la que está en capacidad de comprender.

En la imagen anterior, hemos hecho especial hincapié en describir el dispositivo del lado cliente como "**Modem/Router ADSL**", esto se debe a que en realidad estos dispositivos cubren una doble función, por un lado realizan toda la labor de modulación y demodulación específica de cada extremo de ese par de cobre (*modem*), y por otro lado también trabajan a nivel tres del modelo de capas, es decir, desempeñan actividades de "Routing" (*router*) gestionando y enrutando direcciones y encabezados del protocolo IP del lado LAN (dentro del domicilio) y del lado WAN (hacia la central telefónica a través del par de cobre). Cabe mencionar que en la jerga telefónica la "acometida" en cada hogar, es decir, el punto de entrada de cada domicilio (o edificio) se denomina **PTR** (Punto Terminal de Red) pues es allí donde se encuentra el eslabón final de cualquier operador.

Como es natural, desde el lado de la central, no se pueden colocar 10.000 modem diferentes, sino que se diseña un nuevo hardware que centraliza esas líneas y así nace el **DSLAM** (Digital Subscriber Line Access Multiplexer (Multiplexor de línea de acceso de abonado digital).

A continuación se presenta una visión más amplia de los componentes fundamentales de toda esta red que permite la navegación por Internet a cualquier abonado que tenga ADSL en su domicilio. En la misma solamente se aprecian los elementos base de esta arquitectura pero, como es de suponer, en cada "nube" del esquema se encuentra una cadena/jerarquía de dispositivos que permiten al interconexión y el routing de cada paquete que circula por ella, como así también una

serie de dispositivos y plataformas que forman parte de los procesos de facturación, autenticación, monitorización, supervisión, etc.

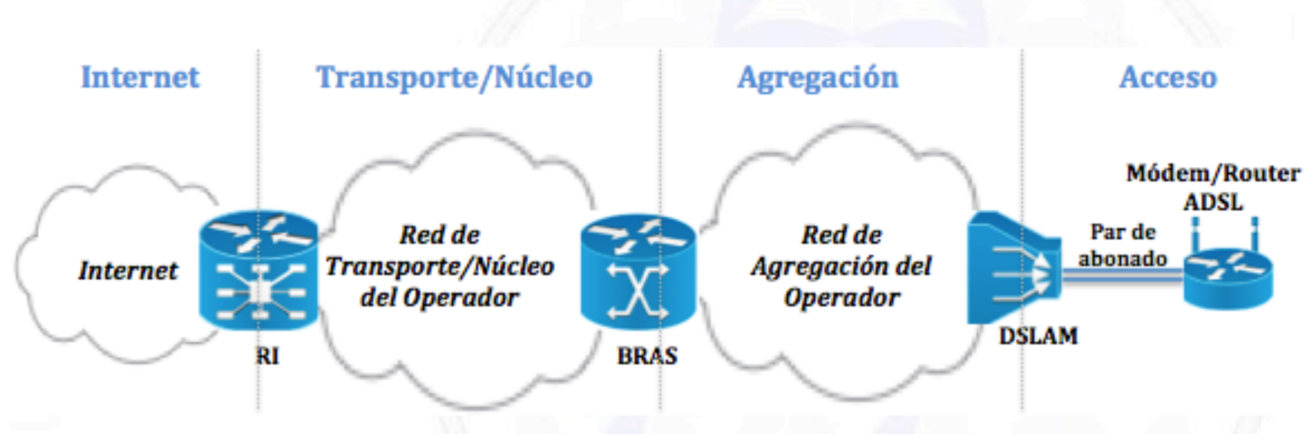


Imagen 1.5 (DSLAM - BRAS)

En la imagen anterior, podemos ver también otro dispositivo que es el **BRAS** (Broadband Remote Access Server) que es elemento de agregación de dos o más DSLAM hacia la red IP de la operadora telefónica. Este dispositivo no deja de ser un router más, sobre el cual se pueden configurar determinados parámetros de administración de banda ancha y protocolo IP.En la actualidad, con la difusión y reducción de precio de la fibra óptica (FO), en las nuevas instalaciones, se está llegando hasta el domicilio del cliente con la misma, se denomina **FTTH** (Fiber To The Home), siempre y cuando hasta ese barrio ya exista FO (denominado **FTTN**: Fiber To The Neighborhood). Es importante tener en cuenta que la relación que existe entre la red fija y la móvil se está haciendo cada vez más competitiva, pues hoy en día se están ofreciendo velocidades por aire de la misma magnitud que las de cable de cobre (*cuestión inimaginable hace una década*). A esta realidad se suma la aparición de teleoperadoras locales y operadores móviles virtuales que lanzan al mercado planes muy tentadores. Para mantener a sus clientes, las empresas que poseen un alto número accesos a la red fija, en las zonas donde su cableado es antiguo o en nuevos barrios, están desplegando fibra óptica de forma masiva, a través de la misma se pueden alcanzar velocidades que dejan fuera de competencia a cualquier otro medio o tecnología. Con ello, una vez acometido todo un barrio, es muy poco probable que estos abonados desistan de su uso en virtud, justamente, de todos los servicios de calidad que le llegarán a su hogar: Voz, datos y video de alta definición.

Si se logra llegar con la FO hasta el domicilio del cliente toda la infraestructura es más eficiente, esto impacta también en una reducción de costes para la operadora.

Como hemos mencionado el problema del par de cobre es el denominado "última milla" pues se trata justamente del promedio de las distancias de acometida domiciliaria, es decir los tramos de pares de cobre que van desde la última central hasta los domicilio, oscila en "una milla" (1,6 u 1,8 km dependiendo si es milla náutica o terrestre), las distancias máximas que se pueden llegar con estos pares de cobre no pueden superar los cinco kilómetros.



En el caso de las fibras ópticas, estas distancias medias son de diez kilómetros, por lo tanto donde antes debía colocar unas 20 o 30 centrales telefónicas, esto mismo se logra con una sola central de fibra óptica, también otra razón de máxima importancia es que los tendidos de cobre son "**auto-alimentados**" pues a través del par de abonado viaja también tensión eléctrica que alimenta los teléfonos, este abastecimiento de tensión hace que en cada central se necesite instalar una infraestructura de alimentación importante: Redundancia de acometida, sistemas de cableado adicionales, Power Bank (Baterías), grupos electrógenos, reguladores, transformadores, combustible, etc. Todo esto es innecesario en fibra óptica.



La red fija, como acabamos de ver, se divide a través de los filtros (o Splitter) desde el domicilio y la primer central urbana, en "Voz" y "Datos". Toda la infraestructura de voz no es motivo de este texto, los aspectos de seguridad de redes los basaremos principalmente en todo lo relacionado al protocolo IP, por lo tanto pasaremos directamente a tratar la parte de datos, y más adelante la parte de voz pero sobre IP (VoIP).

Ya hemos desarrollado la arquitectura actual por medio de la que un abonado accede a la red, basándonos en la "Imagen 5 (DSLAM - BRAS)", nos podemos dar una idea clara de este circuito. Avancemos ahora al detalle de cómo en la realidad, las diferentes empresas de Telefonía, tienen desplegada esta arquitectura.

Como idea básica, partiremos de cuatro conceptos:

- Red de acceso
- Red da agregación (o BakHaul)
- Red de Transporte
- Core de paquetes (Back Bone o núcleo)

En general podríamos afirmar que casi todas las operadoras responden a este tipo de esquemas (y veremos que también aplica a la red móvil), tal vez la única de esta cuatro que puede obviarse en algunos casos es la red de Transporte, cuyo concepto para nosotros será la que se emplea para interconectar regiones geográficas distantes (Provincias, comunidades autónomas, regiones, etc.).

La red de acceso, podemos entenderla como aquella en la que interactúa en parte el usuario final y es la frontera de la operadora hacia el lado cliente. En el caso de la red fija, estaría limitada desde las DSLAM hacia fuera.

La red de agregación, para nosotros será una "Concentración" de varias redes de acceso, es una red intermedia entre los accesos y el Back Bone de la operadora. Su traducción es "red de retorno" y un poco viene a cuento del flujo sanguíneo, que forma este tipo de concentración de los capilares hacia las venas principales.

Y el Core, muchas veces llamado Packet Core (o PaCo), como su nombre lo indica es el corazón de estas redes, por esa razón es que desde el punto de vista de la

seguridad es sin duda el más importante, sin él es imposible ningún tipo de transmisión.

A continuación de los DSLAM un dato que nos interesa es cómo se están organizando en la actualidad estos segmentos de agregación, pues en estos momentos estamos viviendo la evolución de dos tecnologías:

- ATM (asynchronous Transfer Mode).
- MAN Ethernet.

Las redes **MAN** (Metropolitan Área Network) , en las infraestructuras, no son más que "redes de Agregación" (Backhaul). En general veremos dos tipos de tecnologías: ATM y Ethernet (dos protocolos que compiten hace varios años), seguiremos viendo este tipo de arquitecturas durante un tiempo más, es decir la forma en la que se van "sumando" (agregando) históricamente fueron evolucionando desde tramas E1 (aún existentes), pasando por ATM y llegando al día de hoy con las redes Metro Ethernet (A veces también llamadas **MEN**: Metro Ethernet Network) que es la tecnología actualmente dominante. Se trata de un nuevo resurgimiento de esta tecnología Ethernet, que al igual que el ave Fénix, no deja de sorprendernos y que hoy supera los 10 Gbps arrasando cualquier otra competencia. Encontraremos este tipo de redes de agregación en casi todas las operadoras telefónicas.

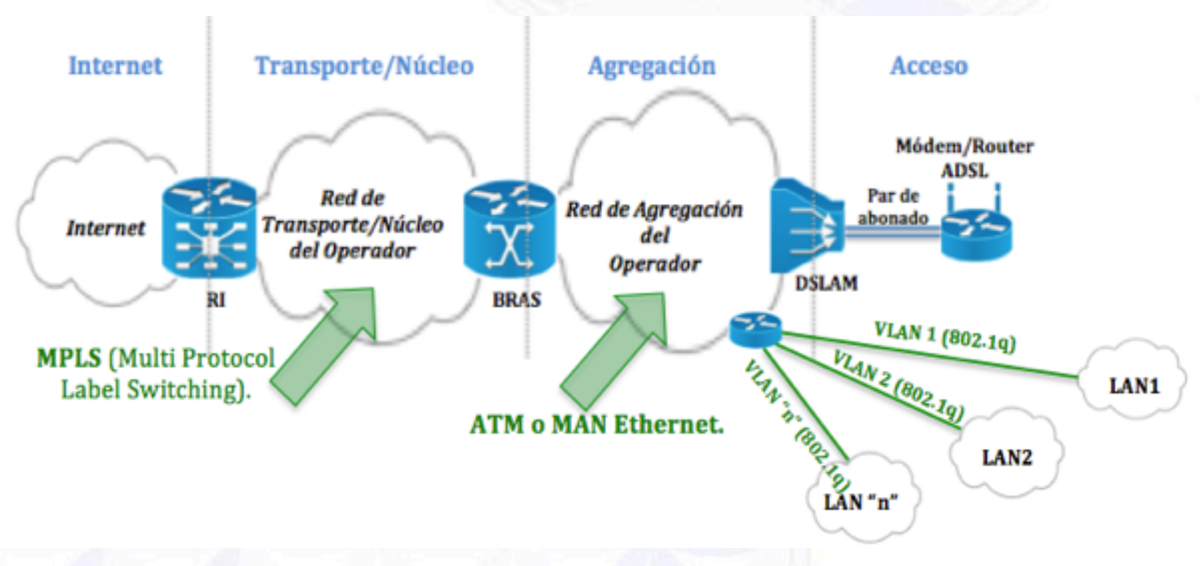


Imagen 1.6 (VLAN y MPLS)

En la figura anterior ampliamos un poco más la visión de estas arquitecturas de red para poder presentar gráficamente dos protocolos que no podemos dejar de lado. El primero está relacionado a la red de acceso. Por este segmento no solo ingresan usuarios domiciliarios, sino también empresas que contratan vínculos de mayor ancho de banda y servicios especiales (*mayor direccionamiento IP, direcciones IP fijas, servicios de voz, de monitorización y soporte, correo electrónico, aplicaciones, etc.).* Este tipo de accesos se suelen incorporar a través de routers dedicados a empresas, existiendo varias parejas de estos routers distribuidos en las diferentes zonas

geográficas y ciudades de cada operadora. Cuando una empresa tiene más de una sucursal, el tráfico interno entra cada una de ellas viaja por toda la infraestructura de la operadora y, como es normal, no desea que su tráfico pueda ser mezclado u observado por otras empresas, por lo tanto para el ingreso de las mismas se suelen emplear **VLAN** (Virtual LAN). La tecnología VLAN está soportada por el protocolo **IEEE 802.1q**, que por ahora solo lo mencionamos para comprender su aplicación en este caso, pero más adelante lo veremos en detalle cuando tratemos "switching". Este protocolo es un gran pilar desde el punto de vista de la seguridad en redes. Cabe mencionar también que este concepto de VLAN se suele emplear también para separar los tráficos de voz, datos, servicios, gestión, etc.

El segundo aspecto importante que deseábamos destacar es cómo en la actualidad se está tratando el tema de conmutación de paquetes a nivel "Core". Debemos considerar que en este segmento de la red es donde se concentra el tráfico que proviene de todos sus extremos y desde aquí es donde se interconecta todo ello con el resto del mundo, por lo tanto es donde mayor ancho de banda se necesita. El protocolo mas difundido en el núcleo de grandes redes suele ser **MPLS** (Multi Protocol Label Switching), que como su nombre lo indica se trata de un protocolo que opera a nivel 2 (Switching), "etiquetando" (label) cualquier protocolo que provenga de niveles superiores, que en nuestro caso suele ser IP (o ATM que está desapareciendo). A través de estas etiquetas, digamos que "baja" a nivel dos el procesamiento de encabezados, logrando mucha más velocidad y redundancia de rutas. Una de las razonas por las que queríamos presentarlo dentro de esta arquitectura completa de red fija es porque ofrece de forma nativa la posibilidad de "inyectar" en el Core a través de lo que se denomina **VRRP** (Virtual Router Redundancy Protocol) las diferentes VLAN que recibe desde las redes Ethernet (LAN o MEN) manteniendo su separación de extremo a extremo. También lo desarrollaremos más adelante.

1.2. La red móvil

El origen de la red móvil para la transmisión de datos es bastante reciente. En la actualidad podemos hablar de las siguientes metodologías:

- **GSM**: (Global System for Mobile Communications, u originariamente: Groupe Special Mobile - 2G), el acceso era exactamente igual que el de cualquier teléfono fijo, es decir a través de un modem analógico con una limitada velocidad, por esta razón es que nos centraremos en los servicios de telefonía móvil que fueron pensados no para redes analógicas, sino digitales y con la oferta de conmutación de paquetes, de los cuales el primero fue GPRS y luego UMTS. Velocidad máxima para transmisión de datos: 9,6 kbps
- **GPRS** (General Packet Radio System – 3G). Velocidad máxima para transmisión de datos: 171,2 kbps aunque en la práctica no suele pasar de 40 kbps de bajada y **de 9,6 kbps de subida.**

- **UMTS** (Universal Mobile Telecommunications System – 3.5 G). Velocidad máxima para transmisión de datos: 2 Mbps.
- **LTE** (Long Term Evolution – 4G). Velocidad máxima para transmisión de datos: en bajada: 326,5 Mbps para 4x4 antenas y 172,8 Mbps para 2x2 antenas, en subida: 86,5 Mbps.

En el ámbito hispano para el que está escrito este libro, si bien puede existir algo de CDMA (Acceso múltiple por división de código) en algún segmento de alguna operadora en particular, su presencia en España y Latinoamérica es ínfima, por lo tanto no lo desarrollaremos.

La lógica de esta conexión de datos inalámbrica, se inicia cuando un dispositivo desea realizar una comunicación de datos sobre la red (es decir se conecta a través de un modem de datos digital). Esta comunicación, a diferencia de la de voz, a grandes rasgos se establece con un primer nodo de la red telefónica que a partir de 3G se denomina **GGSN** (Gateway GPRS Support Node), entre ambos se inicia el establecimiento de una relación denominada **PDP** (Packet Data Protocol), que de tener éxito finaliza con la creación de un "Contexto PDP" bajo el cual ya se establecieron todos los parámetros de seguridad y direccionamiento para que ese móvil pueda navegar por la red. No merece la pena entrar en más detalles al respecto, tampoco profundizar sobre el dialogo PPP o L2PP o el protocolo IP para Móviles (MIP), etc.

Las redes 2G y 3G.

A continuación presentamos imágenes de cada una de estas tecnologías:

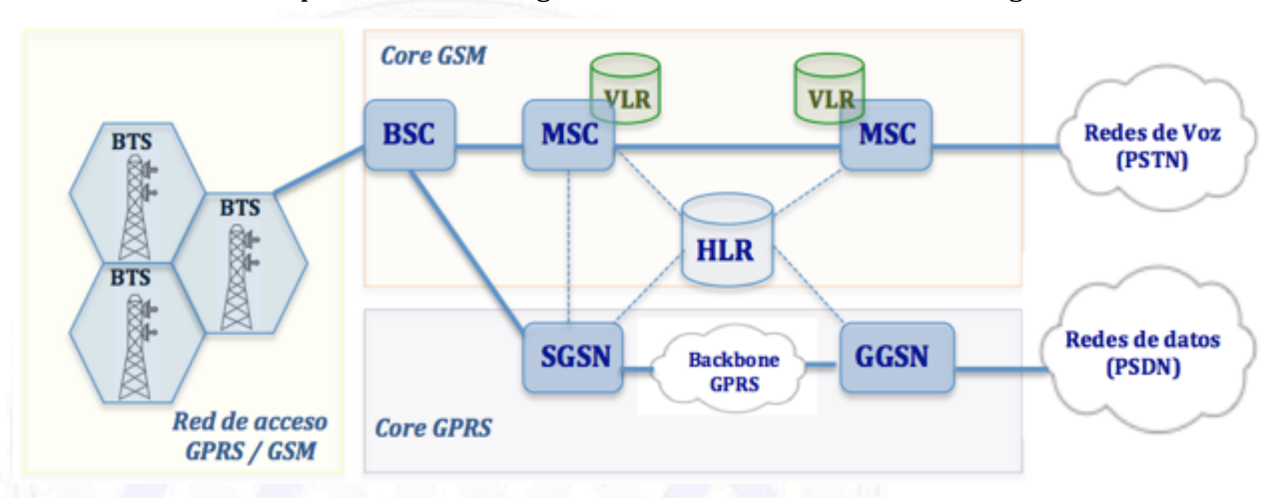


*Imagen 1.7 (Arquitectura **GSM** y **GPRS**)*

En la imagen anterior estamos presentando las tecnologías 2G y 3G, podemos diferenciar tres grandes rectángulos:

Amarillo: *A la izquierda.*

En esta zona podemos ver las diferentes celdas o células que están siendo cubiertas por las antenas o **BTS** (Base Transceiver Station). Cada operadora Nacional, oferta sobre los diferentes espectros que el País saca a licitación, una vez ganadas y adjudicadas estas licencias, se planifica la distribución de

celdas para dar cobertura en el territorio que haga falta (actividad sumamente compleja), cada celda debe tener un ancho de banda y una potencia de emisión tal que no se solape con las celdas aledañas y es gobernada por una BTS. Se debe tener en cuenta también que dentro de todo este cálculo no es lo mismo la distribución de celdas en centros urbanos de alta concentración, donde en muchos casos llegan a existir más de una celda por manzana, y como se verá más adelante también instalaciones de lo que se conoce como "Small cells", en contrapartida con las zonas rurales donde una misma celda cubre varios kilómetros a la redonda.

En el caso de las tecnologías GSM y GPRS, ambas comparten la misma zona de acceso.

Naranja: *Arriba y a la derecha.*

Este es el Core de GSM, esta zona no tiene capacidad para diferenciar entre voz y datos, toda esta infraestructura de tráfico aún no opera por paquetes por lo tanto toma todos los flujos como "Voz", por esa razón es que como se mencionó anteriormente, para las aplicaciones de datos se empleaba un modem analógico, hoy prácticamente como tecnología de datos está en desuso, por ello no merece la pena detenernos más. Como podemos apreciar está compuesta de varios dispositivos:

- **BSC** (Base Station Controller): Es la entidad controladora de varias celdas y se encarga del control general de los recursos radio proporcionados por una o varias BTSs.
- **MSC** (Mobile Switching Center): Es la central que realiza todas las funciones de señalización y conmutación requeridas para el manejo de servicios de **CS** (Circuit Switching) hacia y desde una determinada área geográfica. La principal diferencia con una central de una red fija es que incorpora funciones para la gestión de la movilidad como los procedimientos para el registro de posición y para el handover (Cambios de celdas).
- **HLR** (Home Locator Registry): El HLR es una de las piezas fundamentales de la telefonía móvil, contiene una base de datos encargada de gestionar los abonados móviles. Una operadora puede poseer uno o varios HLRs. El HLR almacena información de subscripciones y datos de ubicación que permiten la facturación y encaminamiento de llamadas/mensajes hacia el MSC/SGSN donde se ha registrado la MS. Como podemos ver en la imagen, las líneas que unen a este dispositivo no las hemos graficado como continuas, sino "punteadas", esta suele ser una representación muy habitual en redes para identificar que por ese camino no circula información de usuarios (voz o datos) sino información de "**control o señalización**".
- **VLR** (Visitor Location Register): Se encarga de controlar la itinerancia. Cuando un teléfono móvil entra en una nueva celda, se comienza un procedimiento de registro. El MSC o SGSN encargado de dicha área notifica este registro y transfiere al VLR la identidad del área de ubicación donde la **MS** (Mobile Station, teléfono móvil) está situada. Si dicho móvil no esta todavía registrado, el VLR y el HLR intercambian información para permitir el adecuado manejo de las

llamadas del mismo. El VLR puede estar encargado de una o varias áreas MSC o SGSN.

En la imagen anterior, ya podemos apreciar dos caminos diferentes. La parte superior izquierda, nos muestra la interfaz radio que comparten ambas tecnologías (GPRS/GSM), es la misma para ambas, pero en la parte inferior derecha ya se pone de manifiesto toda esta nueva infraestructura que aparece con GPRS para la transmisión exclusiva de datos (SGSN y GGSN). Ahora la BSC, es la responsable de "dividir" estos flujos: en el caso de voz mantiene la conmutación de circuitos por medio del MSC y en el caso de datos, opera por medio de conmutación de paquetes entregándoselos al SGSN.

Hay dos dispositivos fundamentales que no hemos graficado en la imagen anterior pues, en general, se encuentran "embebidos" o integrados dentro del HLR, pero que desempeñan una función muy específica, estos son:

- **AuC** (Authentication Center): Contiene una base de datos que mantiene los datos de cada abonado móvil para permitir la identificación internacional de abonados móviles (IMSI) para poder realizar la autenticación del abonado y para poder cifrar la comunicación por el camino radio entre el teléfono móvil y la red. El AuC transmite los datos requeridos para la autenticación y cifrado a través del HLR hasta el VLR, MSC y SGSN que necesitan autenticar al abonado móvil. El AuC almacena claves de identificación para cada abonado móvil registrado en el HLR asociado (Son copias de la clave que está en la SIM de cada móvil).
- **EIR** (Equipment Identify Register): Contiene una base de datos que mantiene los identificadores internacionales de equipos móviles (IMEI) para controlar el acceso a la red de los equipos móviles (listas blancas y negras) de cada "aparato". Es como el número de serie de cada dispositivo móvil que responde a un formato internacional y que identifica unívocamente al teléfono (No a la SIM, ni al número personal que tengamos asignado por la operadora, sino al equipo en sí), por esta razón es que es importante registrar la compra de estos dispositivos y denunciar el robo, pues los diferentes gobiernos a través de sus secretarías de telecomunicaciones (con sus más y sus menos) velan para que las operadoras de su País lleven actualizadas las listas negras de dispositivos robados para evitar este tipo de hechos. Durante este proceso de autenticación de un teléfono móvil con el HLR, un paso necesario es la consulta de este IMEI contra las listas negras que posee el EiR, si este aparato móvil figura en ellas, automáticamente se debería cortar el acceso a la red.

Lila: *Abajo y a la derecha*

Con la aparición de la tecnología 3G se crea un nuevo "core de paquetes" para las redes de telefonía móvil, se mantiene toda la infraestructura de acceso, pero se incorporan estos dos nuevos dispositivos que veremos a continuación:

- **SGSN** (Serving GPRS Support Node): Sigue y mantiene la posición de las MSs en su área, y realiza funciones de seguridad y control de acceso. El SGSN establece contextos **PDP** (Packet Data Protocol) activos que son usados para el encaminamiento con el GGSN que el abonado este usando. La función de registro de posición en un SGSN almacena información de subscripciones y datos de ubicación (Ejemplo: la celda o área de encaminamiento donde la MS esta registrada, o la dirección del GGSN donde exista un contexto PDP activo) de los abonados registrados en el SGSN para servicios con conmutación de paquetes. Dicha información es necesaria para llevar a cabo la transferencia entrante o saliente de datos en paquetes.
- **GGSN** (Gateway GPRS Support Node): Se encarga del funcionamiento entre redes externas con conmutación de paquetes a las que se conecta a través del interfaz Gi (ej: Internet), está conectado con uno o varios SGSNs a través del interfaz Gn. La función de registro de posición en un GGSN almacena información de subscripciones y datos de encaminamiento (ej: la dirección del SGSN donde el MS esta registrado) para cada abonado que tenga al menos un contexto PDP activo. Dicha información es recibida desde el HLR y el SGSN, y es necesaria para poder establecer un túnel de tráfico de datos en paquetes (Túnel GTP), destinado a una MS, con el SGSN donde el MS esta registrado. El SGSN y el GGSN contienen funcionalidad de encaminamiento IP y pueden estar interconectados por routers IP.

Por último, a la derecha de toda la imagen anterior, podemos ver como cada uno ed los Core tiene conectividad con su red correspondiente de forma independiente:

- Core GSM → Red de voz (PSTN: Public Switching Telephone Network).
- Core GPRS → Red de datos (Public Switching Data Network).

Las redes **3,5 G**

La siguiente evolución de la tecnología GPRS fue un cambio substancial de la interfaz de acceso radio. Se diseñó una nueva arquitectura con elementos de acceso que ofrecían mayor ancho de banda en esta zona llegando a los 2 Mbps, esto es lo que se denominó **UMTS** (Universal Mobile Telecommunications System). En la imagen que sigue podemos ver en la parte inferior izquierda (en verde) estos nuevos dispositivos.

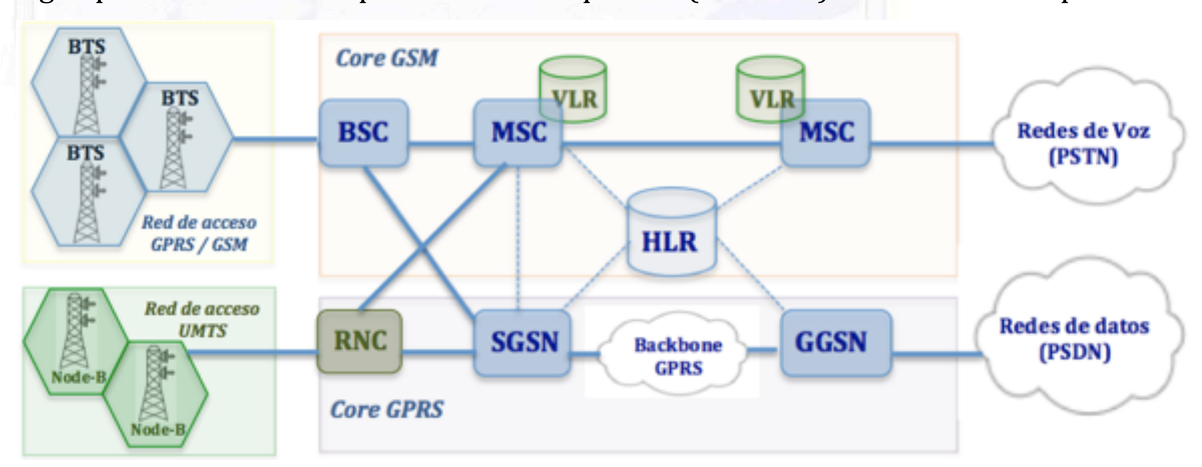


Imagen 1.8 (Arquitectura **UMTS**)

- **Node B** (Nodo B): Es el componente responsable de la transmisión/recepción radio hacia/desde MSs en una o más celdas UMTS. Los nodos B se conectan a los RNCs.
- **RNC** (Radio Network Controller) El RNC es la entidad controladora y se encarga del control general de los recursos radio proporcionados por uno o varios nodos B. El RNC es responsable de las decisiones de handover que requieren señalización al teléfono móvil.

Las redes 4G.

La nueva generación denominada 4G viene implementada a través de la tecnología que se conoce como **LTE** (Long Term Evolution). La arquitectura LTE presenta una serie de cambios de denominación, configuraciones y elementos.

Lo que debemos tener especialmente en cuenta es lo siguiente:

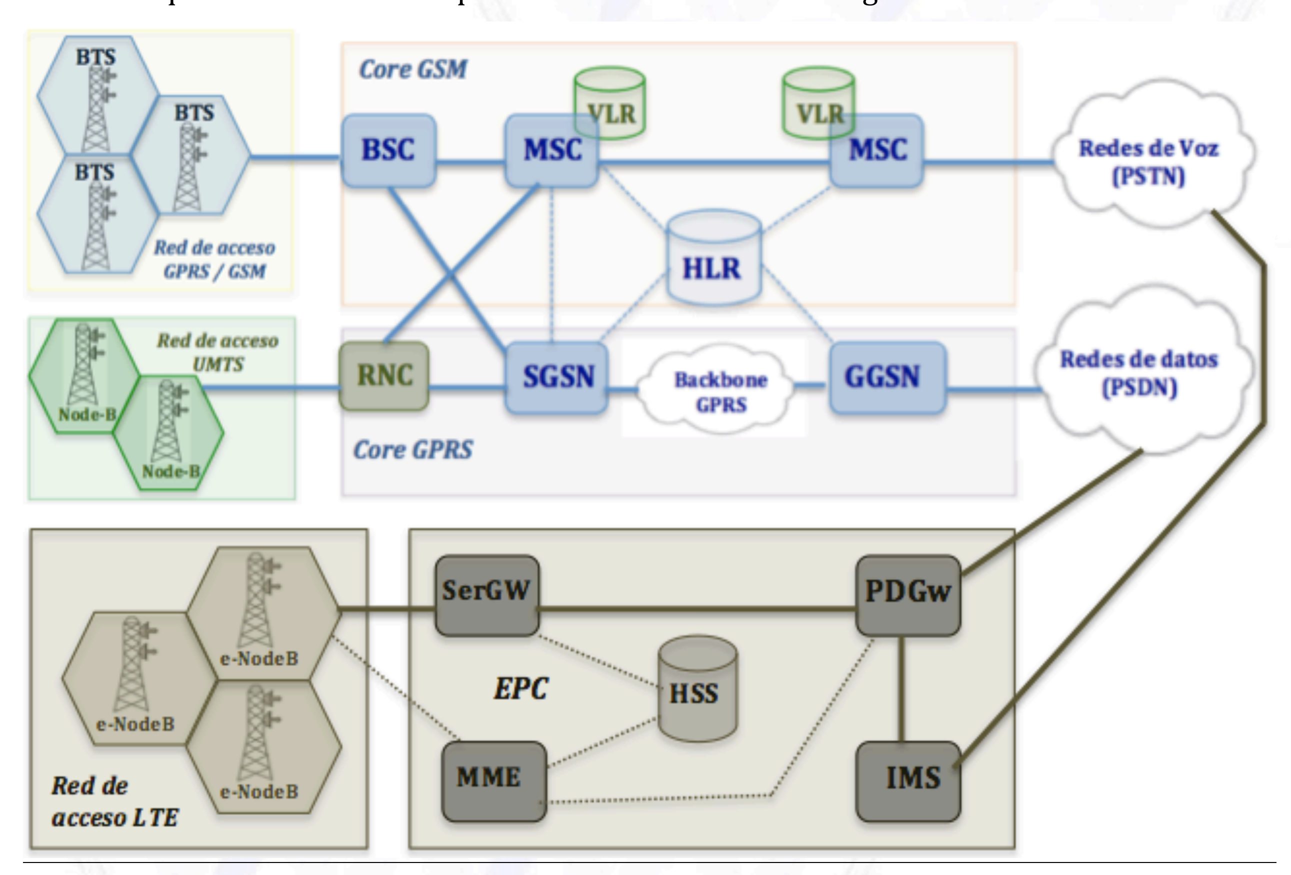


Imagen 1.9 (Arquitectura **LTE**)

Como podemos ver en la parte inferior de la imagen (y en marrón), aparece un nuevo elemento denominado "**eNodeB**" en LTE y el mismo incorpora las funciones de RNC (Radio Network Controller) que ya no existe. Por otro lado como también se puede apreciar que las funciones básicas del SGSN y el GGSN (y otras más también)

quedan cubiertas ahora por lo que se denomina **MME** (Mobility Management Entity) y **SerGW** (Serving Gateway). No hemos querido profundizar en mayores detalles, pues existen varios dispositivos que no hemos puesto para simplificar el concepto, pero sí hemos destacado dos componentes más que serán las piezas clave para recibir paquetes IP y diferenciar el tráfico de voz y datos, que luego deberán encaminar hacia ambas redes exteriores, pues como es natural, en la actualidad y por muchos años aún seguirán existiendo dos "mundos de dominio público", el de voz (PSTN) y el de datos (PSDN). El responsable final de encaminar los datos será el **PDGw** (Packet Data Gateway), mientras que el que "convertirá" paquetes de voz en "flujos" de voz será el **IMS** (Internet Multimedida Subsystem) que desarrollaremos más adelante. Por último vemos que aparece el **HSS** (Home Subscriber Server) que hereda las funciones del HLR, este almacena y gestiona el perfil del servicio IMS del abonado, guarda las claves de seguridad y genera vectores de autenticación, registra el estado de los abonados y almacena el nodo con el que el abonado se ha registrado, etc.

Lo que debemos destacar es que en un único dispositivo se incorporan funcionalidades que implican un hardware y software para optimizar el rendimiento de la interfaz radio. Este nuevo diseño es tal vez el aspecto más importante de LTE, pues desde aquí ya se ingresa a la red con protocolo IP, permitiendo que sea una arquitectura "**all IP**" de extremo a extremo, a una velocidad de subida y bajada nunca antes alcanzada.

El **eNodeB** lleva incorporada la antena y la inteligencia que antes controlaba la RNC (que ahora no existe más) por lo tanto en la mayoría de los casos quedará fuera del dominio de seguridad físico de la operadora, es decir en edificios, locales, áreas rurales o desatendidas, azoteas, túneles, puentes, etc. Es aquí donde se presenta un nuevo desafío de seguridad pues toda esta labor que realiza, implica desarrollos de software a los cuáles se puede acceder por protocolo IP y a su vez este dispositivo para poder ser configurado, posee interfaces físicas de acceso a las cuáles cualquiera también podría potencialmente tener acceso.

Por tratarse LTE de una tecnología en plena fase de despliegue en todo el mundo, a continuación abordaremos el tema de la seguridad de la misma con mayor grado de detalle que las anteriores, pues como se verá están surgiendo bastantes problemas, brechas o debilidades en sus implantaciones.

Los ataques a este nuevo elemento de radio (eNB) pueden realizarse de forma local o remota.

Al obtener acceso físico al eNodeB, cualquier intruso podría interceptar, modificar o inyectar tráfico en la red. Si se presentara esta situación, sería posible todo tipo de manipulación sobre la información de usuario y señalización entre la estación base y el Serving Gateway o también entre las diferentes estaciones base.

Estos requerimientos de seguridad están especificados en la cláusula 5.3 del **TS33.401**.

Como podemos ver en la imagen anterior, una estación base se conecta al **EPC** (Evolved Packet Core), esto lo hace a través de la interfaz que se conoce como "**S1**" y a las estaciones base adyacentes a través de la interfaz "**X2**". La cláusula mencionada del

documento anterior establece los mecanismos de confidencialidad, integridad y antiréplica a emplear en ellas que no todas las operadoras cumplen.

Lo que debería ser común en todos los planos de seguridad de esta especificación es el empleo del protocolo IPsec en modo túnel con empleo de **ESP** (Encapsulation Security Payload) y también el empleo de autenticación con **IKEv2** (Internet Key Exchange) con certificados. La discusión está en que la norma de 3GPP que es el organismo que más peso tiene en las regulaciones y estándares de telefonía móvil deja esta condición como "Opcional", debido a esto es que por razones de costes en general no se está cumpliendo de forma estricta.

Esta especificación técnica, al establecer que tanto para el plano de control como para el de usuario en las interfaces S1 y X2 el modo transporte de IPsec sea opcional, se nos presentan dos problemas:

1) En la transmisión de la información:

- Administración de claves dentro de la estación base.
- La transferencia de datos cifrados (o no) en el plano de usuario entre el e-nodoB y S1/X2 no está explícitamente tratado en esta especificación.

2) En el "Hardening" (bastionado) del "eNodeB":

La especificación menciona el concepto de "entorno seguro" y describe algunas características, de las cuales las más importantes a destacar son:

- Arranque seguro (Integridad del SW).
- Se deja librado a los fabricantes sus sistemas operativos; particionado, formateado discos, aplicaciones, etc. Por lo tanto depende de cada uno de ellos el nivel de seguridad de sus elementos.
- No requiere evaluaciones de seguridad de SW o HW de los fabricantes.
- No requiere medidas de seguridad físicas para el eNB.
- La única especificación que menciona es el concepto de HeNB (Home eNodeB).

Descripción más concreta del problema específico de la nueva tecnología de acceso.

La arquitectura general de LTE se denomina **SAE** (System Architecture Evolution). Esta debe soportar el acceso de todo tipo de redes, dando origen a un nuevo concepto que se está llamando "**HetNet**" (Heterogeneous Networks), concretamente este hecho se está llevando a la realidad, por medio del acceso a través de redes WiFi y/o WiMAX a este EPS, este tipo de acceso se está haciendo habitual en zonas públicas, pues para la operadora es una forma de alivianar sus celdas en zonas de alta concentración y a su vez para ofrecer mejor calidad de servicio a sus abonados. También se está dando con la oferta de "Small Cells" que son antenas de menor cobertura, por medio de lo que se denominan "pico, micro y femto cells" que se comercializan para empresas y también para descongestión de las celdas convencionales (también llamadas Macro cells).

Dentro de estos accesos heterogéneos o HetNets, pueden existir algunos "confiables" y otros "no confiables". Los primeros simplemente son aquellos en los

que el operador 3GPP confía en la seguridad de la red o dispositivo que está accediendo a su Core (como es el caso de las redes CDMA), y los segundos como, una red "no confiable" pueden ser, por ejemplo, el uso de una **WLAN** (Wireless LAN) en un café público o un aeropuerto para conectarse al servicio de red privada (o VPN) de su empresa.

Para todo el proceso de autenticación, existe una importante diferencia cuando un usuario accede al SAE por una u otra de estas redes, y nuevamente nos encontramos que las operadoras por cuestiones de coste, intentan economizar sobre los dispositivos y medidas de seguridad a adoptar.

Resumen de aspectos principales de Seguridad en el acceso LTE:

a. La conexión de los eNB es directa al Core abriendo nuevas posibilidades (interfaces Si y X2).
b. El empleo cada vez más frecuente de micro, pico y femtoceldas incrementa la cantidad de puertas de acceso.
c. El crecimiento de las celdas compartidas entre operadores para minimizar costes.
d. Empleo de otras interfaces de acceso hacia la red (WiFi, WiMAX)

Por qué es importante el empleo de los túneles Ipsec en LTE.

Como ya hemos mencionado, el nuevo factor clave que nos trae el despliegue de LTE está relacionado a este tipo de túneles y el bastionado de los eNB.

La razón de este concepto pasa en particular por la facilidad que ahora puede tener cualquier intruso en acceder físicamente a uno de estos dispositivos (edificios, vías públicas, locales expuestos, etc.). Una vez que accedemos al e-nodoB, estos dispositivos obligatoriamente necesitan tener interfaces físicas de conexión (RJ45, USB, puertos serie), al poder conectarse físicamente a cualquiera de estos puertos, en realidad estamos directamente accediendo al core de la red, pues en "jerga de IP" es nuestro siguiente salto.

Cualquier tipo de instalación de eNB, sea una pequeña o pico celda, o sea una celda completa siempre tendrá una parte de potencia de radiodifusión y otra que es el HW/SW específico de los planos de control y usuario hacia el core de la red.

En la fotografía de la derecha podemos ver los dos módulos bien diferenciados, las tres antenas en la parte superior y la electrónica por debajo.



Imagen 1.10 (Componentes de un enodo-B)

El módulo de HW/SW es la verdadera "inteligencia" del eNB, y es allí justamente donde encontraremos interfaces físicas para conectarnos.

El empleo de túneles IPsec, es el único método para que a pesar de poder acceder físicamente a estas interfaces no pueda continuar el avance hacia el core de red, por supuesto siempre y cuando el nivel de bastionado de este eNB sea el adecuado.

El conjunto de servicios que IPSec puede proveer incluye:

- Control de accesos.
- Integridad no orientada a la conexión.
- Autenticación de origen de datos.
- Rechazo o reenvío de paquetes.
- Confidencialidad.
- Negociación de Compresión IP.

En lo que nos interesa respecto a la seguridad, todo esto lo realiza por medio de los componentes fundamentales de esta arquitectura que son:

- Protocolos de seguridad: Compuestos por **AH** (Autentication Header) [RFC-4302] y **ESP** (Encapsulation Security Payload) [RFC-4303].
- asociaciones de seguridad (**SA**: Security association).
- **IKE** (Internet Key Exchange) [RFC-7296 y 7427], para intercambio de claves manual y automático.
- Algoritmos de autenticación y cifrado.

Para la configuración de los túneles IPec, es necesario el empleo de un dispositivo intermedio denominado **SecGW** (Security Gateway). Un SecGW aparte de ofrecer la ejecución de túneles IPSec, ofrece también la posibilidad de administración de sesiones, control de flujo y control de carga, aspectos muy importantes en la etapa de despliegue de VoLTE, aunque no sean estas las funciones primarias de este dispositivo.

¿Por qué el empleo de IKE y porqué de versión 2 en LTE?

Como acabamos de desarrollar, el empleo de túneles IPsec nos facilita las mayores ventajas desde el punto de vista de seguridad, en particular si a su vez se emplean certificados digitales, pero aún nos queda pendiente el método que emplean ambos extremos para generar claves criptográficas que le permitan "tunelizar" (confidencialidad, integridad, etc..) toda la información transportada y generar la asociación de seguridad.

Para ello el método **Diffie-Hellman** (debido a Whitfield Diffie y Martin Hellman) propone una idea sinceramente "brillante" para poder definir un secreto dentro de un medio público. Dicho en palabras sencillas:

Imaginaros una habitación llena de gente. En un extremo de la misma "A", y en otro extremo "B" desean a viva voz establecer una palabra secreta sin que ninguna otra persona pueda enterarse……….. la propuesta de Diffie-Hellman da solución para este problema basándose en propiedades matemáticas.

En el libro "**Seguridad por Niveles**" en pa parte que desarrollamos los métodos de autenticación y no repudio", se describe con todo detalle el mismo.

Por qué versión 2.

a. IKEv2 proporciona una mejor resistencia a los ataques. IKEv2 puede mitigar ataques de **DoS** (Denegación de Servicio) mediante la validación del iniciador de IPSec.

   Para hacer esta vulnerabilidad difícil de explotar, el que responde puede pedir una cookie al iniciador para asegurarse que es una conexión normal.

   En IKEv2 las cookies del respondedor mitigan el ataque de DoS, ya que este no guarda al estado de la conexión de IKE, ni tampoco realiza la operación de D-H a menos que el iniciador devuelva la cookie enviada por el respondedor.

   El respondedor usa un mínimo de CPU y no creará una SA (asociación de Seguridad) hasta que valide al iniciador.

b. IKEv2 reduce la complejidad en la creación de IPSec entre diferentes equipos VPN. Aumenta la interoperabilidad y permite tener una forma estándar para métodos de autenticación existentes.

   IKEv2 provee interoperabilidad de IPSec entre diferentes vendedores al ofrecer tecnologías como Dead Peer Detection (**DPD**), NAT Transversal (Network Address Translation-T), contacto inicial, etc.

c. IKEv2 contiene menos encabezado, con esto mejora el tiempo de respuesta en el establecimiento del SA. Múltiples peticiones son permitidas (por ejemplo: se crean en paralelo SA subordinadas).

d. IKEv2 reduce el tiempo de SA. En IKEv1, el retraso de la SA, aumenta conforme el volumen del paquete aumenta. IKEv2 mantiene el mismo tiempo aunque el volumen aumente. La creación de SA en IKEv2 tardan menos que en IKEv1.

e. IKEv2 requiere de un menor tiempo para realizar el rekey (regeneración de la llave). IKEv1 toma más tiempo para realizar el rekey que IKEv2. Debido a la redefinición de ciertos mecanismos de IKEv1 (como son, tamaño de ToS, tiempo de vida del SA y singularidad del SPI), en IKEv2 menos paquetes son perdidos o duplicados. Por lo tanto hay menos necesidad de realizar un rekey.

Las redes 5G.

Dentro de 3GPP ya se está hablando y desarrollando esta nueva tecnología. Se trata aún de una teoría que no ha bajado a definiciones o especificaciones técnicas, pero sí se ha puesto como fecha el año 2020 para que esta red móvil ya tenga un desarrollo maduro.

Los aspectos básicos que ya se propone son:

- Nuevas bandas de frecuencia en las que poder operar a nivel radio (entre los 26 y 38 GHz).
- Varias tecnologías de radio soportadas por el estándar (Multi RAT).
- Mayores velocidades (más de 7 Gbps).
- Personalización de los servicios para cada aplicación específica.

- Mayor cantidad de terminales a las que pueda dar servicio cada antena de forma simultánea.
- Menor consumo de energía en los terminales.

1.3. Las redes de voz y datos

Como hemos vista a lo largo de los puntos anteriores, la historia de las redes de grandes operadoras nacieron de forma separada como redes de voz y de datos, también se encuentran bastante segregadas las redes fijas de las móviles.

Las tecnologías de fibra óptica para la red fija y LTE para la red móvil, nos llevan a un paradigma donde no tiene sentido tratar de forma diferenciada los conceptos de voz y datos. Las redes de conmutación de paquetes, a pesar de ser "no orientadas a la conexión", "no confiables" "sin entrega ordenada", hoy en día ofrecen una velocidad de transmisión tan excesivamente alta, y una tasa de errores tan baja que pueden ofrecer servicios de voz de mayor calidad aún que las redes de conmutación de circuitos.

Todo acceso de fibra óptica implica que desde el router domiciliario en adelante TODA la voz viaja paquetizada, es decir sobre protocolo IP, este hecho lo desarrollaremos en breve.

La red LTE que en realidad debería ser también "all IP" y por lo tanto la voz también sobre IP, aún no cumple este concepto en gran parte del mundo, pues para las comunicaciones de voz (con excepción de muy pocas operadoras en pocos países del primer mundo) se realiza lo que se denomina "Callback", es decir las llamadas vuelven a la generación anterior, y en vez de ser voz sobre LTE (VoLTE) sigue siendo voz sobre GPRS (VoLGA)

La realidad es que el despliegue de VoLTE requiere una calidad de servicio y parámetros de latencia que no son sencillos de alcanzar, para poder cumplir con el lanzamiento de LTE al menos para ofrecer altas velocidades de datos es que se opta por continuar dividiendo los caminos de voz y datos con esta solución conocida como VoLGA que es la que se presenta a continuación:

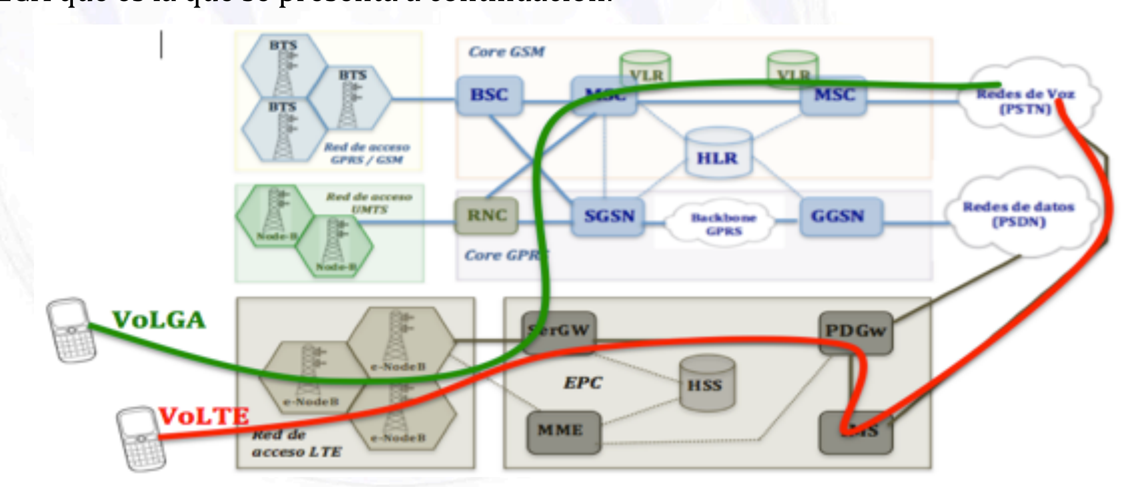


Imagen 1.11 (VoLGA y VoLTE)

VoLTE (Voice over LTE) - **VoLGA** (Voice over LTE vía Generic Access)

Como se puede apreciar en la ruta verde, cuando la operadora no posee la infraestructura para ofrecer VoLTE, el Serving Gateway al detectar que se trata de una comunicación de voz, debe conmutar la misma a la arquitectura de GPRS, tomando el control de la comunicación el MSC y siguiendo el camino de cualquier comunicación 3G.

En el caso de la ruta verde cuando se trata de una comunicación de voz, es el mismo PDGw que recibe los paquetes y los deriva a la infraestructura de IMS que procesa esa información y lo deriva hacia la red pública de voz directamente. Cabe aclarar aquí que si la operadora que gestiona la ruta completa de la comunicación hasta el otro extremo, también poseyera infraestructuras de voz paquetizada, todo este camino sería "all IP", cosa que aún no ocurre a nivel "Inter Operadoras" de Telefonía. El detalle de estas comunicaciones de voz sobre IP lo trataremos, dos secciones más abajo.

1.4. Internet

En este apartado, no dedicaremos tiempo a historia de esta red o aspectos conocidos de su evolución, sino a la descripción técnica que nos hace posible hoy en día poder transmitir información por todo el mundo.

Hemos visto someramente los diferentes tipos de acceso e infraestructuras básicas que nos permiten conectarnos a la red e inclusive parte de estas zonas, plataformas e infraestructuras que poseen las operadoras nacionales que en definitiva son las que llegan a través de la red fija o móvil hasta cada uno de nosotros, clientes finales. Avancemos ahora más en profundidad sobre los detalles de estas conexiones.

Si comenzamos a analizar esta red de forma jerárquica desde arriba hacia abajo, lo primero que nos encontramos son los grandes "Carriers" del mundo, es decir los que interconectan continentes y países de forma bastante piramidal. Existen tres niveles de ellos, conocidos como Tier 1, Tier 2 y Tier 3.

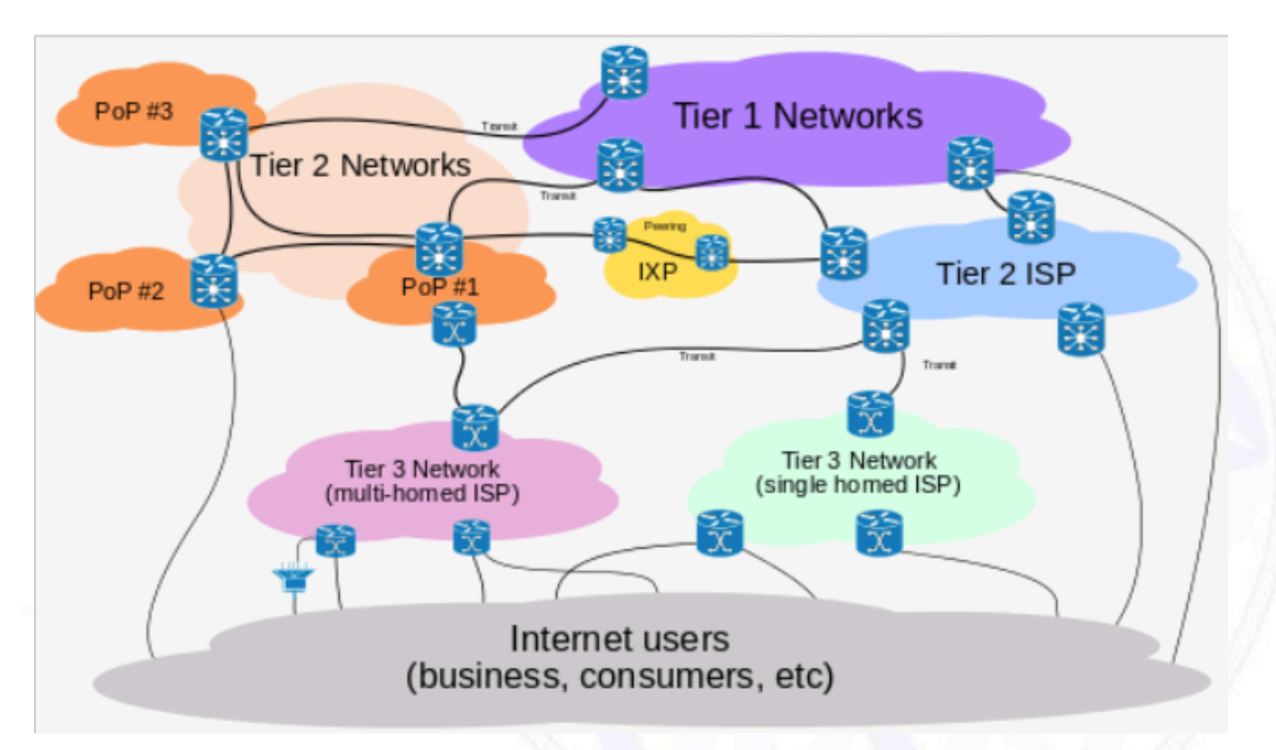


Imagen 1.12 (Tiers de Internet) (Imagen tomada de Wikipedia)

Los **Tier 1** son los grandes operadores globales que tienen tendidos de fibra óptica al menos a nivel continental. Desde la red de un Tier 1 se accede a cualquier punto de Internet, pues todas las redes de Tier 1 deben estar conectadas entre sí. Son backbone, core, núcleo ó troncal de Internet. Si bien se puede llegar a discutir la frontera entre algún Tier 1 específico, los que podemos considerar sin lugar a dudas como Tier 1 son:

Nombre	Sede	Nº as (asN)
Cogent anteriormente PSINet	Estados Unidos	174
Level 3 Communications (Ex Level 3 y Global Crossing)	Estados Unidos	3356 / 3549 / 1
XO Communications	Estados Unidos	2828
AT&T	Estados Unidos	7018
Verizon Business (anteriormente UUnet)	Estados Unidos	701 / 702 / 703
CenturyLink (anteriormente Qwest and Savvis)	Estados Unidos	209 / 3561
Sprint	Estados unidos	1239
Zayo Group anteriormente AboveNet	Estados Unidos	6461
GTT (anteriormente Tinet)	Estados Unidos	3257
NTT Communications (anteriormente Verio)	Japón	2914
Teliasonera International Carrier	Suecia - Finlandia	1299
Tata Communications (adquirió Teleglobe)	India	6453
Deutsche Telekom (Hoy: International Carrier Sales & Solutions)	Alemania	3320
Seabone (Telecom Italia Sparkle)	Italia	6762
Telefónica	España	12956

Independientemente de su magnitud, también deben reunir algunas características como son:

- Deben tener acceso a las tablas completas de routing a través de las relaciones que poseen con sus peering (otros tiers).
- Deben ser propietarios de fibras ópticas transoceánicas y enlaces internacionales.
- Deben poseer redundancia de rutas.

El dato más representativo y actualizado del peso y actividad de cada uno de ellos se puede obtener a través de CAIDA (Center for Applied Internet Data Analysis) en:

http://as-rank.caida.org

Un ejemplo cercano de Tier 1 lo tenemos con Telefónica, a través de su empresa **TIWS** (Telefónica International Whole Sales) o actualmente con su nuevo nombre **TBS** (Telefónica Bussiness Solutions), desde su página Web podemos apreciar el mapa que se presenta a continuación donde se presentan todas los vínculos físicos que controla este Tier 1.



Imagen 1.13 (Red Internacional del Grupo Telefónica) (Imagen tomada de la web: http://www.internationalservices.telefonica.com)

Los máximos niveles de estos "Carrier", en realidad no conocen el detalle de las direcciones IP, sino que sus rutas se gestionan dinámicamente a través del concepto de Sistemas Autónomos (**as**: Autonomous System). Estos as se identificaban con un número (**asN**: as Number) que se asigna a través de **IANA** (Internet assigned Numbers Authority), que ocupaba 16 bit (dos octetos, por lo tanto no más de 65.535 posibilidades). En el año 2007, en virtud de la saturación de los mismos se publicó la **RFC-4893** *"BGP Support for Four-octet as Number Space*", que actualmente ha quedado obsoleta y reemplazada por la **RFC-6793** del mismo nombre y que define el empleo de 32 bit para el espacio de asNs. Estos números son asignados en bloques (por parte de IANA) a los diferentes Registros Regionales de Internet (**RIR**: Regional Internet Registry), estos son:

- **ARIN** :American Registry for Internet Numbers (América del Norte).
- **RIPE-NCC**: Réseaux IP Européens Network - Coordination Centre (Europa, el Oriente Medio y Asia Central).
- **APNIC**: Asia-Pacific Network Information Centre (Asia y la Región Pacífica).
- **LACNIC**: Latin American and Caribbean Internet Address Registry (América Latina y Caribe).
- **AfriNIC**: African Network Information Centre (África).



Los diferentes RIRs son los que finalmente asignan los asNs a grandes empresas de telecomunicaciones, universidades, organismos oficiales y de internet.

Imagen 1.14 (RIRs) (Imagen tomada de Wikipedia)

La definición clásica de un Sistema Autónomo deberíamos acordarla según lo que establece la RFC-4271 y resumidamente es: *"conjunto de routers bajo una única administración técnica que utiliza un protocolo interior (denominado **IGP**: Interior Gateway Protocol) y una métrica común para determinar cómo enrutar los paquetes dentro del AS y fuera del mismo hacia otros ASs"*

La gestión de estas rutas se realiza de forma dinámica a través del protocolo BGP (Border Gateway Protocol) que actualmente se regula por la mencionada RFC-4271 "A Border Gateway Protocol 4 (BGP-4)", y es el responsable de mover la totalidad de las rutas para alcanzar todos los ASs. Los Tier 1, son los únicos que comparten las tablas completas de ruteo a través de este protocolo, manteniendo permanentemente, y con copias exactas en cada uno de ellos los caminos "troncales" de Internet, estas se conocen como **RIB** (Routing Information Base). Este intercambio de rutas, se realiza a través de conexiones TCP sobre el puerto 179.

Tal vez la mejor web para investigar protocolo BGP y ASs es: http://www.he.net (Hurrican Electric), allí podemos encontrar todo tipo de información técnica actualizada, o reportes que necesitemos para investigar sobre estos temas.

Las redes Tier 2 son operadores de ámbito más regional que no pueden alcanzar todos los puntos de Internet y que necesitan conectarse a una red Tier 1 para ello. Su principal función es ofrecer servicios de conectividad a los operadores Tier 3. En esta categoría ya no ponemos ejemplos pues son muchos más

Las redes Tier 3 son los **ISP** (Internet Service Providers) que dan servicio de acceso a Internet domiciliario y a empresas. Los ISPs, en general coinciden con las operadoras nacionales (pero no tiene por qué ser así), son los que nos "abrirán las puertas" hacia Internet.

Siguiendo con la lógica de este texto, nos quedaría desarrollar la "Conexión" entre esta red "fija" y esta red "móvil" que presentamos en los puntos anteriores con Internet.

Quedamos en que la red fija a través de sus segmentos de acceso, agregación y transporte llega hasta el Core de red, por otro lado la red móvil con su GGSN o PDGw derivarán sus paquetes de datos hacia las "redes de datos", en ambos casos cada uno de estos paquetes confluirán en lo que se suele denominar "Packet Core" (o PaCo), que en algunas operadoras telefónicas ya está unificado para fija y móvil y en otras aún no, pero esta integración no nos debe interesar para comprender estas arquitecturas. Lo que sí es importante es cómo cada operadora enruta su tráfico de clientes hacia el resto del mundo. Para esta tarea tenemos básicamente dos escenarios:

- Interconexión con su "Carrier" (Salida Internacional): En este caso se trata de routers del ISP, que físicamente están conectados a routers de un "Tier 1 o Tier2" y entregan su tráfico para que ellos lo enruten a través de Internet. Este tipo de enlaces suelen ser redundantes y en general hacia al menos dos Carriers diferentes par garantizar su disponibilidad.

- Punto de Intercambio (**IXP**: Internet eXchange Point): Se debe considerar que el tráfico de Internet, tiene un alto porcentaje que se mantiene dentro de las fronteras de cada país (consultas a Web nacionales, correos locales, etc..), este tipo de tráfico no tiene sentido que sea enrutado fuera de estas fronteras pues sobrecargaría las troncales de la red. Para estos casos en muchos países (no todos) se han creado estos IXP, que en definitiva son salas con "Racks" de comunicaciones (básicamente switchs de alta capacidad) donde se interconectan los grandes carriers de ese país. Al organizarse las rutas BGP, es natural que este tipo de enlaces ofrezcan mayor ancho de banda que si siguieran otros caminos, por lo tanto a la hora de generarse las tablas de ruteo, el "peso" que tienen estos caminos supera cualquier otro, debido a ello se generan rutas locales preferenciales que encaminan el tráfico nacional, sin la necesidad de salir de ese país.

1.5. Voz sobre IP y VoLTE

El tema de Voz sobre IP, generalmente abreviado VoIP (Voice Over IP), debe ser presentado marcando bien la diferencia entre cualquier servicio de VoIP y la nueva tecnología de 4G que emplea Voz sobre LTE, que se denomina VoLTE (Voice Over LTE).

Para ofrecer VoIP sólo hace falta poder digitalizar los 4 KHz del canal vocal de nuestro dispositivo de entrada (micrófono, teléfono, etc..) en un canal básico de 64 kbps (que luego podrá o no ser comprimido) e inyectarlo como cualquier otro fichero en una red IP. La calidad que se pueda ofrecer sobre esta red es el punto clave.

Hoy en día, cualquier ordenador puede realizar esta digitalización y existen cientos de programas que permiten instalar servicios de VoIP. Si se tiene en cuenta que cualquier red LAN ofrece en la actualidad un ancho de banda mínimo de 100 Mbps y relacionamos esta velocidad con los 64 kbps de nuestro canal de voz digitalizado, estamos hablando de una relación de 1562,5 veces superior (es decir 100.000 % 64 = 1562,5) esto quiere decir que el mismo paquete de voz, podríamos inyectarlo 1.500 veces en la red y así y todo viajar cada uno de ellos más rápido que en un canal telefónico clásico de conmutación de circuitos de 4.000 Hz. Si bien una red de paquetes no nos garantiza la entrega ordenada, y luchará con colisiones para ingresar a esta red LAN, así y todo es tan inmensamente superior la velocidad que nos podemos dar el lujo de reenviarlo cientos de veces hasta que garanticemos la entrega en el tiempo necesario. Es difícil de comprender estas diferencias de velocidad, pues se llega al caso de poder plantear que si hablo a viva voz, mis mensajes viajarán a 300 m/s (velocidad de la onda acústica), pero si el mismo mensaje lo envío por un cable UTP (pares trenzados) o por una fibra óptica, estaría viajando a velocidades que superan los 200.000.000 m/s…… esto implica que si el mismo mensaje que envío a viva voz, a su vez lo ingreso a esta fibra óptica, el mismo podría enviarlo, prácticamente 1.000.000 de veces antes que llegue a la onda acústica a su destino, aunque esté a pocos metros de distancia.

El problema nuevamente será el de calidad de la red, pues si la red LAN está saturada de hosts o tiene un insatisfactorio número de colisiones, esta relación comienza a degradarse. El caso más real es cuando escalamos el entorno de esta red LAN e intentamos transmitir VoIP a través de Internet. En este último caso, nuestros paquetes de voz circularán por los routers que el protocolo BGP tratado recientemente, haya decidido enrutar, y cada uno de estos routers poseerán su propio vínculo, con un ancho de banda diferente y procesarán nuestros paquetes junto a varios millones de millones de paquetes más, de los cuáles algunos poseerán un nivel de calidad o prioridad de servicio mejor o peor, serán descartados, o retransmitidos, etc. Y allí la calidad ya empieza a ser un problema más importante, llegando al extremo que la comunicación vocal sea insostenible.

Algunas empresas han desarrollado sus servicios específicamente para mejorar esta calidad, montando verdaderas infraestructuras propietarias de comunicaciones a través del mundo que hacen un alto esfuerzo para mejorar esta calidad (Skype, WhatsApp, etc.), pero así y todo siempre existirán segmentos de red que quedan fuera

de su jurisdicción y la calidad no llega a ser la óptima, aunque en la actualidad hay que reconocer que están ofreciendo un servicio muy bueno.

Todo esto, sin entrar en los detalles de routing, es resumidamente de lo que se trata VoIP, pero iniciamos esta sección justamente con la idea de marcar la diferencia entre VoIP y VoLTE pues es aquí donde la "Calidad del Servicio" es el punto clave.

Desarrollemos qué es VoLTE.

En el punto "1.3. Redes de voz y datos." Presentamos la imagen 11 (VoLGA y VoLTE) donde graficamos este concepto, pero lo más importante a destacar sobre LTE es que a partir de aquí es "**all IP**", es decir deja de existir la conmutación de circuitos y está TODO paquetizado, tanto voz como datos. Como podemos apreciar en esa imagen aparece el concepto de "**e-nodoB**" en la interfaz radio y el de **EPC** (Evolved Packet Core) conformado por este nuevo despliegue.

El despliegue de VoLTE requiere una calidad de servicio y parámetros de latencia que no son sencillos de alcanzar, para poder cumplir con el lanzamiento de LTE, es normal que las operadoras telefónicas opten por la solución de VoLGA, pero en el corto/medio plazo serán el 100% VoLTE.

Se prevé que casi el 56 % de los suscriptores de telefonía celular relacionada con LTE van a utilizar servicios VoLTE a finales de 2019.

Aunque la red LTE proporciona un marco para la aplicación de QoS al nivel de aplicación, la nueva tecnología de señalización no es una verdadera garantía de la calidad de la llamada. Para garantizar una experiencia valedera del cliente, las operadoras necesitan verificar la calidad real experimentada por los abonados que hayan comprado servicios de VoLTE, para que puedan tomar medidas inmediatas si la calidad no es tan alta como se pretendía o se esperaba. En pocas palabras, existe una diferencia significativa entre la aplicación de la prioridad del tráfico y la verificación de lo que en la actualidad veremos que se denomina "calidad de la experiencia" (QoE) del suscriptor.

Beneficios de VoLTE

VoLTE ofrece importantes beneficios tanto para los usuarios como para los operadores de redes. Un estudio de investigación independiente de Signals Investigación Group analizó el rendimiento de VoLTE en una operación comercial con visibilidad de acceso de radio, básico e **IMS** (IP Multimedia Subsystem), incluyendo la funcionalidad VoLTE primaria. El informe evalúo el tiempo de establecimiento de llamada, la confiabilidad, la calidad, las necesidades de recursos de la red y el impacto sobre la vida de la batería del dispositivo. El estudio arrojó las siguientes perspectivas:

- La calidad de las llamadas de VoLTE superó con creces la de la voz en conmutación de circuitos 3G y fue mensurablemente más alta que el servicio de voz de alta definición que ofrece Skype.
- Con carga de la red (es decir, compitiendo contra alto volumen de tráfico), y en particular con las aplicaciones en segundo plano que se ejecutan en el

teléfono móvil y la transferencia de datos con la red, los resultados de VoLTE fueron considerablemente mejores que los de Skype.

- El tiempo de establecimiento de llamada por VoLTE fue casi dos veces más rápido que para el establecimiento de llamada en 3G (en VoLGA).
- VoLTE utilizó esencialmente menos recursos de red que la voz de Skype, lo que a su vez dio lugar a una vida estimada más prolongada de la batería del dispositivo para el abonado y una red más eficiente para las operadoras.
- Al salir de la cobertura de LTE, las llamadas de VoLTE fueron transferidas con éxito como voz de circuitos conmutados en 3G, asegurando que las llamadas continuaran sin interrupción.

Así, en última instancia los suscriptores se benefician de una experiencia de alta calidad y mayor duración de la batería del dispositivo, mientras que los operadores disfrutan de una mayor eficiencia en la entrega y de suscriptores más felices.

VoLTE se basa en dos normas **3GPP** presentadas por separado: Subsistemas multimedios IP (IP Multimedia Subsystems - **IMS**), introducidos por primera vez en la versión 5 UMTS de 3GPP; y **LTE**, que fue introducida por primera vez en la versión 8 UMTS de 3GPP. IMS no depende de la existencia de LTE ni LTE depende de IMS, pero VoLTE puede ser concebido como un proceso que combina IMS y LTE para crear un entorno capaz de dar soporte a tráfico de voz de alta calidad en una red de paquetes de datos compartida.

La red IMS es la tecnología líder empleada hoy en día para las llamadas VoIP sobre una red LTE en el sentido de que es IMS el que reconoce la necesidad de condiciones especiales de red necesarias para dar soporte al tráfico de voz. La red LTE recibe instrucciones de la red IMS usando el Protocolo de Iniciación de Sesión (**SIP**) como protocolo de señalización, para establecer conexiones de llamada con la QoS apropiada. Con VoLTE, IMS dirige a LTE para establecer el entorno de QoS deseado e inicia la llamada de voz. IMS también notifica a LTE cuando la llamada se ha terminado, y dirige a LTE para que cierre el entorno especial para voz.

Retomando el tema de la calidad, existe un parámetro fundamental denominado “Identificador de clase de QoS” (**QCI**) que especifica el nivel de latencia aceptable para diferentes tipos de tráfico, como se muestra en la siguiente figura, y es descripto en una Plantilla de Flujo de Tráfico (**TFT:**Traffic Flow template) activada por el elemento denominado PCRF que trataremos más adelante.

Esta plantilla es la siguiente:

QCI	Tipo de portador	Prioridad	Retardo de paquetes	Pérdida de paquetes	Ejemplo
1	GBR	2	100 mseg	10^{-2}	Llamada VoIP
2		4	150 ms	10^{-3}	Llamada de video
3		3	50 mseg		Juegos en línea (en tiempo real)
4		5	300 ms	10^{-6}	Transmisión de video por secuencias
5	No GBR	1	100 mseg		Señalización IMS
6		6	300 ms		Video, servicios basados en TCP, por ejemplo: correo electrónico, "chat", ftp, etc.
7		7	100 mseg	10-3	Voz, video, juegos interactivos
8		8	300 ms	10^{-6}	Video, servicios basados en TCP, por ejemplo: correo electrónico, "chat", ftp, etc.
9		9			

La misma "hazaña" podría llevarse a cabo incluso si uno de los dispositivos es un cliente de software VoLTE que se ejecuta sobre un PC.

Abuso de un portador de video

Una situación similar podría presentarse con un portador de video señalado con QCI y dispuesto para transportar tráfico que no es de video. Un portador de video permite tasas de ancho de banda mucho mayores y, en función del plan de tarificación, la red de la operadora podría involuntariamente tasar los datos como cero.

Control de política universal

Hablando en términos UMTS, en 3GPP una TFT es un clasificador que empareja sobre campos en la dirección IP interna de un túnel **GTP-U** (GPRS Tunnelig Protocol - User plane) (o portador dedicado). Ya sea utilizando el modelo TFT estático o el modelo TFT dinámico, se produce la misma secuencia: se crea un portador dedicado (contexto PDP secundario), y el tráfico específico de las aplicaciones es forzado a coincidir con el mismo.

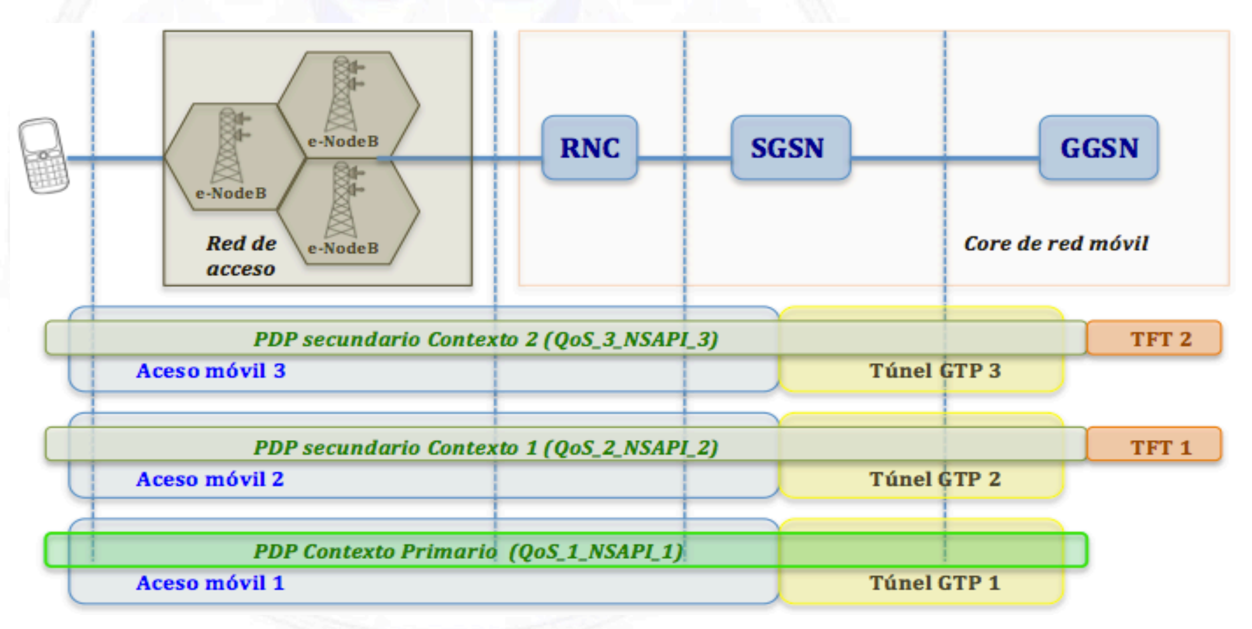


Imagen 1.15 (Diferentes túneles en VoLTE)

La TFT es donde las operadoras crean definiciones sobre cómo será manejado el tráfico de aplicaciones específicas, incluyendo VoLTE, en base a condiciones de política preestablecidas.

Vamos a ahondar un poco más sobre este tema pues aquí subyace un aspecto muy importante desde el punto de vista de la seguridad en VoLTE.

Un portador es un mecanismo de red que permite a la misma sesión de red de acceso celular IP (denominado **CAN**: Cellular Access Network) discriminar tanto la calidad como la tarificación para diferentes aplicaciones. Cuando un dispositivo LTE se conecta a la red por primera vez, se le asigna un "portador predeterminado", que permanece mientras que el dispositivo esté conectado. Los dispositivos pueden tener más de un portador predeterminado, pero cada portador predeterminado tiene una dirección IP diferente y única. El portador predeterminado **no** proporciona Tasa de bits garantizada (GBR), y se pueden especificar valores QCI para No GBR de 5 a 9.

> NOTA: Se resaltan determinados conceptos, porque desde el punto de vista de seguridad, son foco principal de ataques (*muchos de ellos con éxito*) pues obrando convenientemente se logra modificar parámetros de calidad o tarificación de VoLTE con los beneficios (*para el usuario*) y los perjuicios (*para el operador*) pertinentes. *Por supuesto no entraremos en detalles de cómo se realiza esta actividad……*

Un **portador dedicado** es esencialmente un túnel dedicado para una o más aplicaciones específicas (por ejemplo, VoIP, video, juegos, etc.). Un portador dedicado no requiere una dirección IP separada, y utiliza la dirección IP asociada con el portador predeterminado previamente establecido. La TFT se utiliza para especificar la configuración de calidad para una aplicación de tráfico específico transportado sobre un portador dedicado, que puede ser GBR o No GBR en función del valor QCI elegido para dar soporte a un caso de uso específico, como se muestra a continuación:

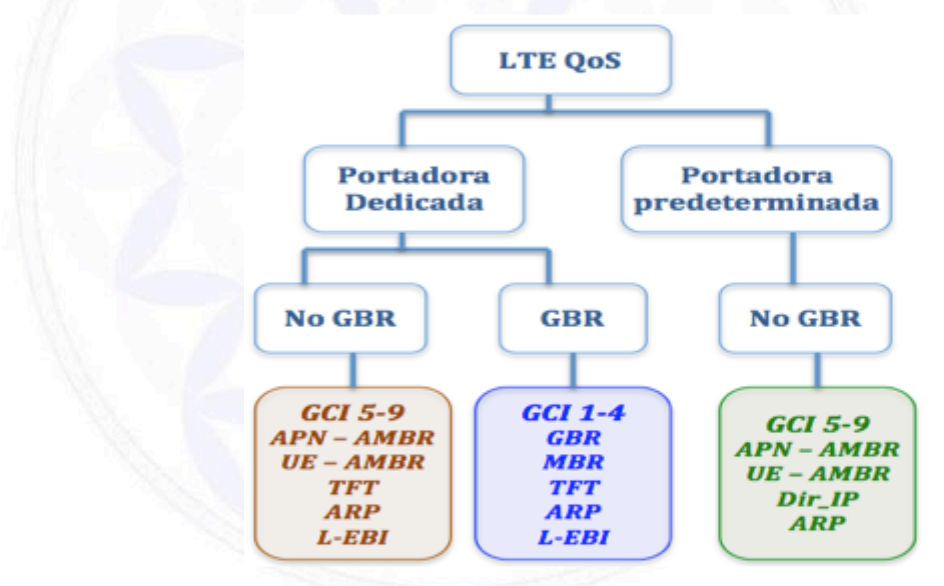


Imagen 1.16 (GBR y No GBR)

En la red con todo en IP, el **portador dedicado determina la QoS** para una aplicación en particular. En el caso de VoLTE, como mencionamos en el punto anterior, la certeza cableada de la red de conmutación de circuitos es sustituida por la garantía de QoS de un portador dedicado con un valor **QCI de 1**. Con VoLTE también existen normalmente dos portadores predeterminados: uno se utiliza para los mensajes de protocolo de inicio de sesión (**SIP**) relacionados con la red IMS (valor QCI de 5), y el otro portador predeterminado, establecido al lograrse la conexión, se utiliza para todos los demás tráficos del teléfono inteligente (video, chat, correo electrónico, navegación, etc.) sobre la red LTE. El componente de señalización **SIP** requiere su propio portador predeterminado (con dirección IP única asociada) porque la red IMS es independiente de la red LTE y viene con su propio **APN** (Access Point Name). Esto también ayuda a estructurar las partes móviles del proceso de acoplamiento IMS-LTE que permite las llamadas de VoLTE.

Flujo de llamada de VoLTE

Cuando un usuario enciende su dispositivo habilitado para VoLTE (por ejemplo, teléfono inteligente), éste se conecta a la infraestructura de la red LTE y se le asignan dos portadores predeterminados **EPS** (Evolved Packet Switch): uno para señalización SIP con un valor QCI No GBR de 5, y otro para la red LTE con valor de QCI No GBR de 5 a 9. Este enfoque de doble portador permite que un teléfono inteligente VoLTE se comunique tanto con LTE como con IMS (SIP).

El flujo de llamadas para habilitar VoLTE se muestra a continuación.

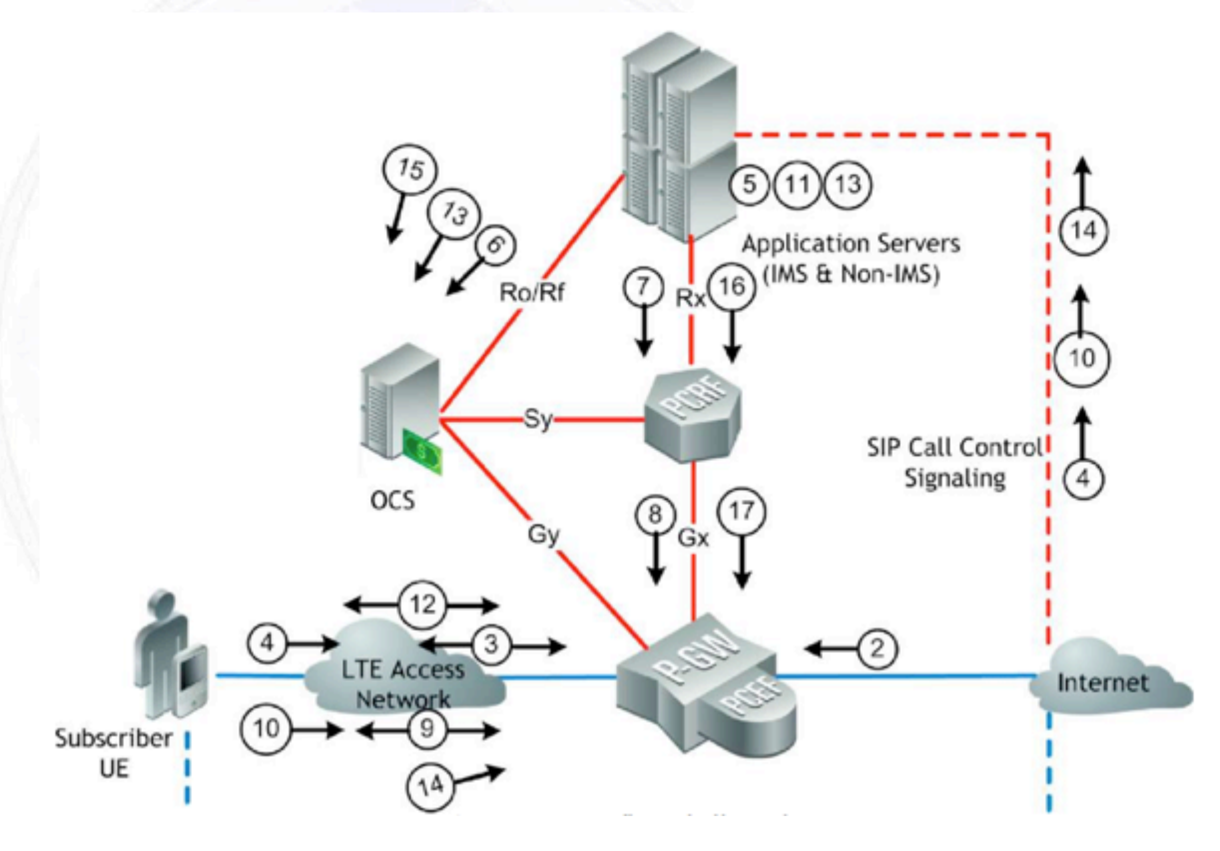


Imagen 1.17 (Secuencia VoLTE)

1) El suscriptor móvil indica en su teléfono inteligente habilitado para LTE el querer hacer una llamada de VoIP.
2) LTE identifica una puerta de enlace ("gateway") PDN (P-GW) que ofrezca una conexión a la red IMS.
3) LTE establece un portador predeterminado para SIP desde el suscriptor hasta la P-GW seleccionada.

   El portador EPS predeterminado es establecido con un valor de Identificador de clase de QoS (QCI) de 5 (el valor de QCI necesario para la señalización SIP).
4) El teléfono inteligente envía un mensaje SIP "Invitar" hacia la red IMS. Un Protocolo de descripción de sesión (SDP) que lleva el requisito sobre QoS está contenido en el mensaje SIP. Tenga en cuenta que aunque los mensajes SIP son transportados a través de la red LTE, la red LTE no es consciente del contenido del mensaje (ni de la necesidad de un tratamiento especial de QoS en esta etapa).
5) La red IMS extrae el ajuste de QoS requerida del mensaje SIP.
6) Si se aplica una política de tarificación, entonces la red IMS envía una solicitud inicial de control de crédito (CCR) de Diameter al OCS, sobre la interfaz Ro y se reserva un monto inicial de crédito anticipando la necesidad de medir con precisión los datos de flujo durante la llamada.
7) El requisito de QoS es enviado desde la red IMS a la PCRF a través de la interfaz Rx (utilizando el protocolo Diameter).
8) La PCRF crea reglas procesables sobre tarificación y calidad de servicio, y las transmite a través de la interfaz Gx a la Función de Cumplimiento de Políticas y Tarificación (PCEF) que reside con la P-GW en la red LTE.
9) Ahora la P-GW envía una solicitud para establecer un "portador dedicado" independiente (con un valor QCI de 1) al teléfono inteligente.
10) Después de que el teléfono inteligente confirma que LTE puede dar soporte al nuevo portador dedicado, envía un mensaje SIP "UPDATE" (actualizar) a la red IMS.
11) La red IMS completa el proceso de configuración y establece la llamada.
12) Los paquetes bidireccionales de llamada VoIP fluyen dentro de la red LTE (a la P-GW) y al teléfono inteligente.
13) Para tarifar, la red IMS solicita crédito al OCS en el transcurso de la llamada (por ejemplo, cada 10 segundos). Si no existe crédito, se devuelve un mensaje 402 (pago requerido) al teléfono inteligente y la llamada es cancelada. Si el crédito expira durante la llamada, ésta se da por terminada.
14) Cuando termina la llamada, el teléfono inteligente envía un mensaje SIP "BYE" (adiós) a la red IMS.

15) La red IMS envía una petición de terminación de CCR en Diameter al OCS, que termina la medición de tarificación y activa las acciones a fin de recolectar los registros de facturación del SIV.
16) La red IMS notifica a la PCRF acerca de la terminación de la llamada.
17) La PCRF indica a la PCEF que cierre la facturación LTE, e instruye a la P-GW a descartar el portador dedicado establecido para la llamada de VoIP.

Un desafío clave propio de VoLTE es el aumento en **más de 10 veces** de la carga de señalización en el plano de control y el elemento PCRF, que debe especificar la QoS para cada llamada de voz individual que pase a través de la red LTE. Cuando se toma en cuenta la adición de servicios de aplicaciones no vocales tales como transmisión por secuencias de video y juegos en línea, la carga de señalización aumenta aún más.

Un informe detallado de Oracle muestra que el tráfico global de señalización Diameter en LTE crecerá a una tasa compuesta de crecimiento anual (CAGR) del **78 %** entre 2013 y 2018, creciendo de 12 millones de mensajes por segundo (MPS) a cerca de 216 millones de MPS.

Prevención del fraude

Existe una verdadera posibilidad de fraude por parte de los usuarios que imitan el marco QCI; al hacerlo, estos usuarios pueden potencialmente solicitar un tratamiento específico de datos no deseados o autorizados por las operadoras.

Abuso del portador VoLTE

Un usuario malintencionado puede establecer un "portador VoLTE" dedicado para transportar tráfico que no es VoLTE mediante la manipulación de las aplicaciones o sistemas operativos en dos dispositivos. Los dos dispositivos podrían teóricamente transmitir cualquier tipo datos de uno al otro. Ya que los portadores VoLTE suelen (o al menos a menudo) ser tasados con cero, entonces este usuario gozaría de datos gratuitos y la operadora perdería ingresos. Además, la elevada tasa de bits alta garantizada para el portador VoLTE también permitiría al usuario malicioso experimentar ancho de banda reservado y calidad protegida para el tráfico que no merece tal tratamiento.

Los operadores de redes convergentes (es decir, aquellos con múltiples tecnologías de acceso) se enfrentan a una serie de desafíos relacionados con la implementación del control de política en toda la red. No es raro que estos operadores tengan una solución para control de política diferente en cada tipo de acceso; Sin embargo, además de la onerosa sobrecarga de capacitación y mantenimiento, este enfoque fraccionado implica que una política única en toda la red (por ejemplo, para habilitar cuotas a través de múltiples tipos de acceso, o para calificar con tasa cero los datos patrocinados) debe ser definida en múltiples ubicaciones, un proceso que es a la vez operacionalmente intensivo y propenso a errores.

La Figura siguiente muestra una red con tres tecnologías de acceso: cable, Wi-Fi y LTE. Normalmente, una red de este tipo tendría al menos dos soluciones separadas para control de políticas: una PCRF para la red LTE (y probablemente para la red Wi-

Fi), y un controlador de política PCMM (PacketCable Multimedia) para la red de cable. Ambos sistemas cumplen las mismas funciones: tomar y hacer cumplir las decisiones sobre políticas.

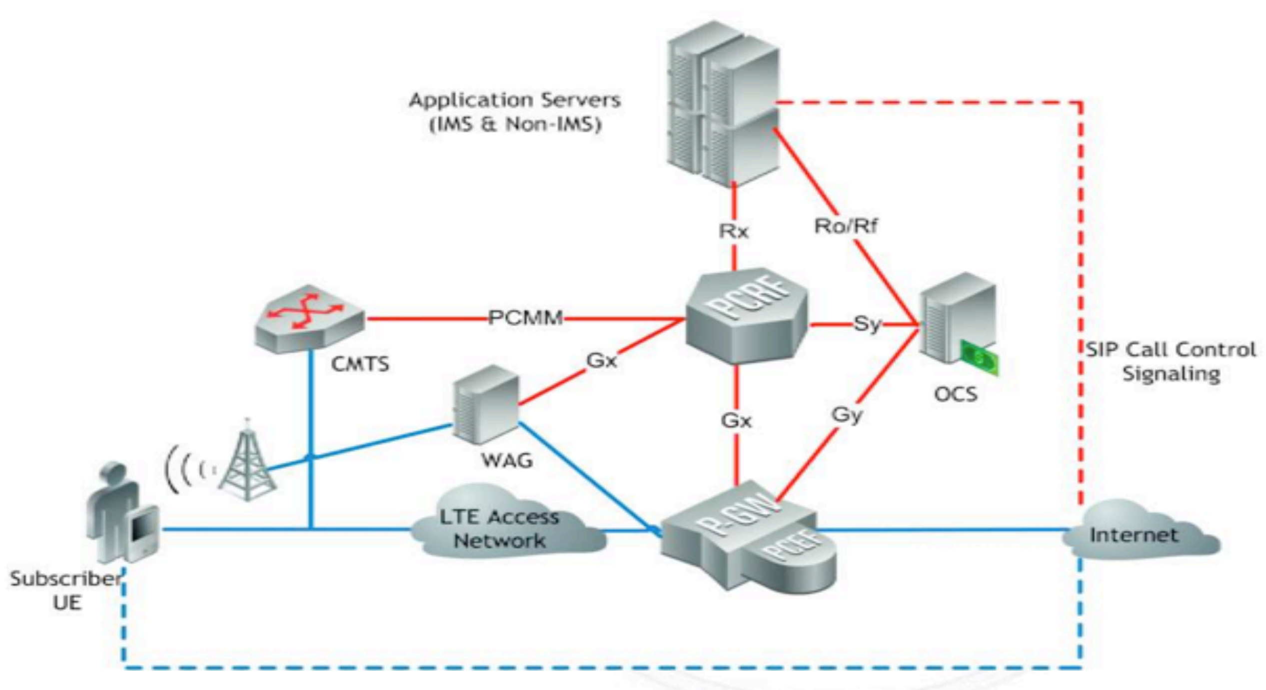


Imagen 1.18 (Secuencia VoLTE)

NOTA: *Uno de los aspectos de especial atención es la situación actual de los despliegues de IMS que veremos más adelante, pues en general en las operadoras de telefonía ya se está empleando esta tecnología de IMS para los accesos de voz fija (FTTH) y en definitiva, este será el mismo IMS que se empleará en un futuro cercano para VoLTE, por lo tanto si hay errores o debilidades de esta infraestructura por confianza en el acceso fijo, este se propagará Voltee.*

1.6. NGN (Next Generation Network)

Como concepto inicial, podemos pensar que NGN nace como una necesidad de ofrecer nuevos servicios cuyo origen es el protocolo IP, pero empleando la antigua red de telefonía conmutado (**PSTN**), que como se ha tratado de ir presentando hasta ahora, no está diseñada para transmitir "paquetes", por lo tanto se hacía necesario implantar esta especie de "parche" particularmente asociado a la señalización de esta red.

Hay varias definiciones sobre NGN, pero en definitiva podemos resumirlas como:

"Red multiservicio (voz, fax, datos y vídeo) integrada para el transporte de paquetes basada en la pila TCP/IP, con posibilidad de diferenciar los flujos de tráfico y ofrecer QoS".

Los puntos fuertes de NGN son:

- Sistemas de transmisión serán de última generación y basados en tecnologías ópticas **WDM** (Wavelength Division Multiplexing).
- Los elementos de conmutación serán de tipo Gigabit Switch-Router (**GSR**) o Terabit Switch-Router (**TSR**), conformando una red IPv4/IPv6 con soporte de **MPLS** (Multi Protocol Label Switching).
- Política de calidad de servicio (**QoS**) efectiva y totalmente operativa.
- Diseño de red escalable que permita evoluciones futuras de forma gradual.

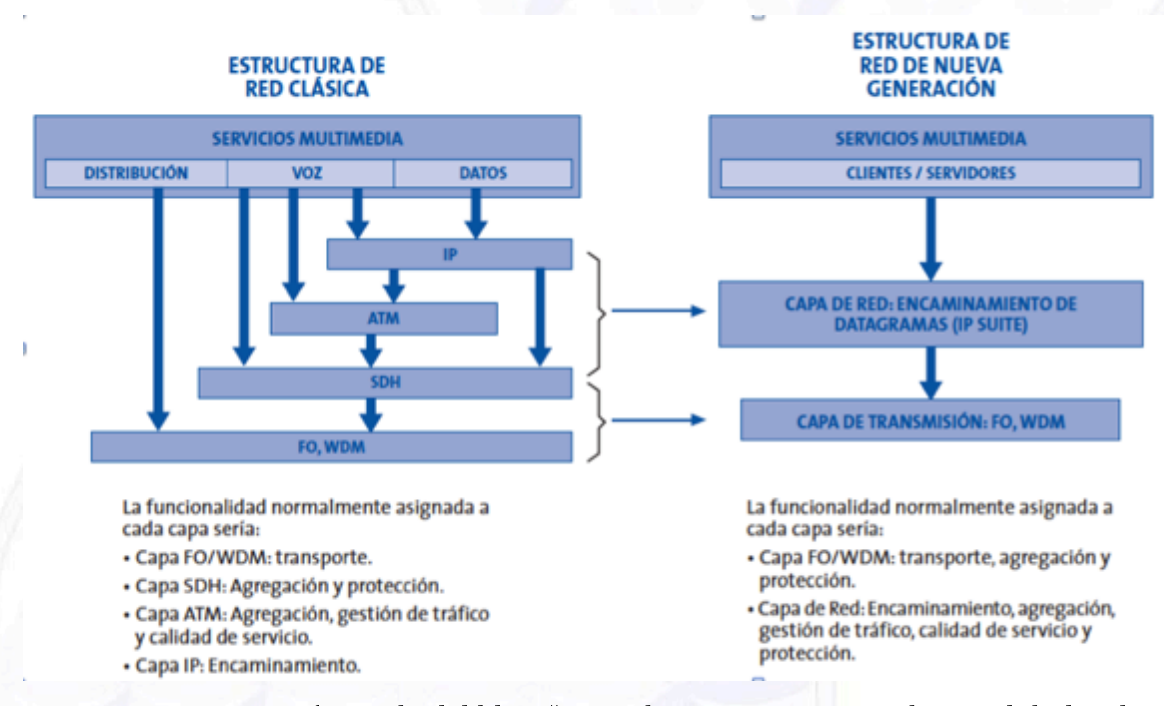


Imagen 1.19 (tomada del libro "Las Telecomunicaciones y la Movilidad en la Sociedad de la Información" - Telefónica)

Otra forma de presentarla es como lo hace **Wikipedia**:

Desde un punto de vista más práctico, las NGN suponen tres cambios fundamentales en la arquitectura de red tradicional que han de ser evaluados de forma independiente:

1) Respecto al núcleo de red, NGN supone la consolidación de varias redes de transporte (dedicadas u overlay) construidas históricamente a partir de diferentes servicios individuales. También implica la migración del servicio de

voz desde la tradicional arquitectura conmutada (PSTN) a la nueva VoIP además de la sustitución de las redes tradicionales (X.25, Frame Relay).

2) Respecto a las redes de acceso, NGN supone la migración del canal tradicional dual de voz y datos asociado a las redes xDSL hacia instalaciones convergentes en las que las DSLAMs integren puertos de voz o VoIP, permitiendo de esta forma dejar atrás las actuales redes conmutadas que multiplexan voz y datos por diferentes canales.
3) Respecto a las redes cableadas, la convergencia NGN implica la migración de la tasa constante de flujo de bits a estándares que suministren servicios **VoIP** y **SIP**.

En NGN existe una **separación** bien definida entre:

la red de transporte (conectividad) ← → Servicios que corren por encima de esa red.

NGN está basada en tecnologías Internet incluyendo el protocolo **IP** y el **MPLS**. En el nivel de aplicación, los protocolos **SIP** parecen haberse incorporado desde la norma ITU-T **H.323**.

NOTA sobre H.323

*H.323 se creó originalmente para proveer de un mecanismo para el transporte de aplicaciones multimedia en LANs, pero ha evolucionado rápidamente para dirigir las crecientes necesidades de las redes de VoIP. Está basado en el protocolo **RDSI Q.931** y está adaptado para situaciones en las que se combina el trabajo entre IP y RDSI.*

*Es utilizado comúnmente para Voz sobre IP (**VoIP**) y para videoconferencia basada en IP. Es un conjunto de normas ITU para comunicaciones multimedia en redes IP.*

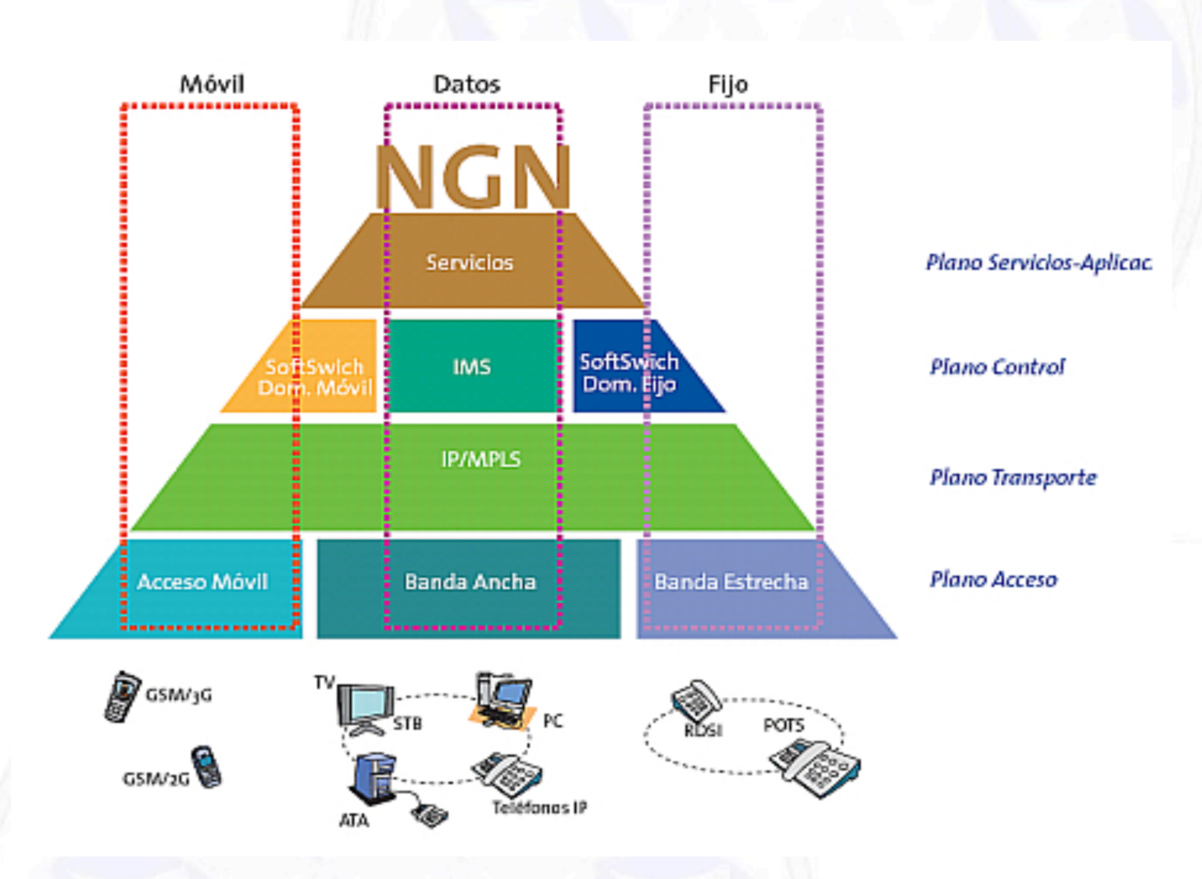
(El siguiente párrafo es fundamental para una estrategia de Seguridad):

*Inicialmente H.323 era el protocolo más famoso a pesar de que su popularidad decayó en la red local **por su pésima gestión de NAT y firewalls**. Por este motivo, los nuevos servicios **SIP** están siendo mejor acogidos. Sin embargo, mientras que en las redes de voz todo el control se encuentra bajo el operador telefónico, la mayoría de los portadores a gran escala usan H.323 como elección más acertada. Por tanto, **SIP** es realmente una herramienta muy útil para la red local y el protocolo H.323 es como la norma para la fibra de transporte. Con los últimos cambios introducidos por el protocolo H.323, es posible que ahora los nuevos dispositivos H.323 soporten la gestión de NAT y firewalls. No obstante, la **mayoría de las operadoras telefónicas están haciendo un estudio intensivo y apoyo hacia el IMS** que da al protocolo **SIP** una mejor oportunidad de ser el nuevo protocolo más utilizado.*

Para las aplicaciones de voz, uno de los dispositivos más importantes en NGN es un **Softswitch**, dispositivo programable que controla las llamadas de voz sobre IP (VoIP). Éste habilita la correcta integración de los diferentes protocolos en la NGN. Su función

más importante es la de crear la interfaz para la actual red telefónica, PSTN, a través de Puertas de Señalización (**SG**: Signalling Gateways) y Puertas Multimedia (**MG**: Multimedia Gateway).

Resumen Final de NGN: Debemos pensarlo como un "importante cambio en la <u>integración multimedia</u> <u>y separación</u> de las capas de **red** de los **servicios bajo filosofía IP**"



<u>Imagen 1.20 (Planos NGN) (tomada de Wikipedia)</u>

Por último el concepto de **IMS** (IP Multimedia Subsystem) que veremos a continuación, <u>es una estandarización de arquitectura NGN</u> para los servicios multimedia de Internet definida por **ETSI** (Instituto Europeo de Estándares de Telecomunicación) y **3GPP** (3rd Generation Partnership Project).

<u>SIGTRAN</u>

No sería adecuado pasar a tratar el tema de IMS sin antes hacer un alto sobre el concepto de SIGTRAN

SIGTRAN (o Señalización de Transporte) es el nombre del grupo de trabajo de la **IETF** (Internet Engineering Task Force) que desarrolló <u>una serie de protocolos</u> que

permiten transportar señalización de control de telefonía pública SS7 y Q.931 por redes IP, fue publicado como el RFC 2719 "*Architectural Framework for Signaling Transport*". Se refiere a una pila de protocolos para el transporte de señalización (SS7/C7) de la red de conmutación de circuitos (**SCN**: Switching Circuit Network) sobre una red IP. Es la evolución natural de **SS7** (Sistema de Señalización número 7).

Con el desarrollo de la telefonía IP, se hacía necesario transportar los **flujos** de señalización sobre redes IP. Al principio las soluciones eran propietarias y fue solo a fines de los '90s que la IETF empezó un esfuerzo por estandarizar estos protocolos. El grupo de trabajo se creó en 1998 y se presentó como la **RFC 2719** "*Architectural Framework for Signaling Transport*" en Octubre de 1999.

Los componentes clave en la arquitectura SIGTRAN son los siguientes:

- Media Gateway Controller (**MGC**), responsable de mediar el control de llamadas (entre la SG y MG) y controlar el acceso del mundo IP hacia y desde la PSTN.
- Signaling Gateway (**SG**), responsable de la interconexión a la red SS7 y la transmisión de mensajes de señalización a los nodos IP.
- Media Gateway (**MG**), responsable de empaquetar de tráfico de voz y transmisión del tráfico hacia el destino.
- Teléfono IP, genéricamente conocido como terminal.

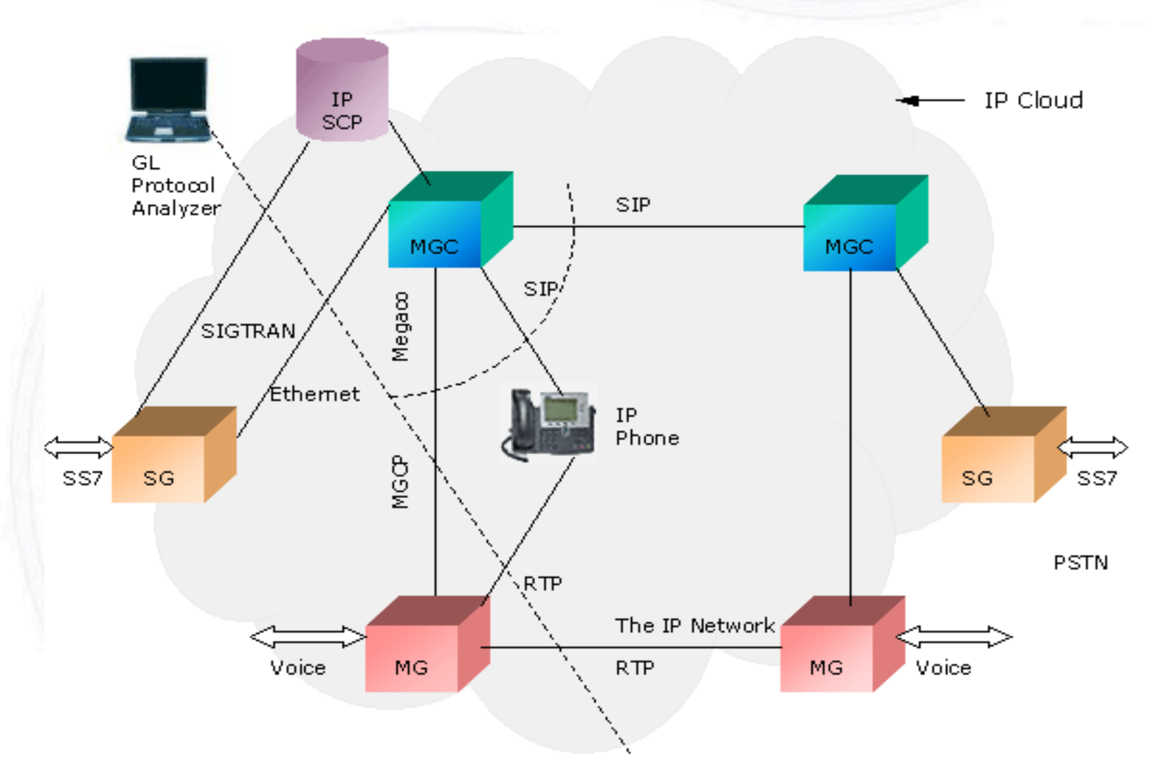


Imagen 1.21 (Señalización)

1.7. IMS (IP Multimedia Subsystem)

Sin entrar en profundidad sobre este subsistema, a continuación se presentan brevemente los aspectos fundamentales para poder comprender qué auditar sobre el mismo.

IMS es la clave tecnológica para diseñar y operar redes basadas en tecnología IP con máxima eficiencia ofreciendo la totalidad de los servicios que se requieren hoy en día y con total independencia del tipo de accesos, sea fijo o móvil.

En estos momentos IMS es imprescindible en toda Operadora pues es la evolución natural de todas las anteriores tecnologías hacia un mundo "all IP". Si bien existieron otro tipo de propuestas, la totalidad de los prestadores de servicios de Internet se han orientado hacia IMS, por lo tanto es la arquitectura líder del mercado.

Para el usuario final, ofrece nuevas opciones de comunicación basadas en sesiones que pueden ser de voz o cualquier otro "flujo" multimedia. Tal vez el hito más significativo es la diferencia conceptual para la Operadora, donde antes cada servicio era independiente de los demás y se necesitaba desplegar infraestructura particular para cada uno de ellos duplicando elementos, con IMS se minimizan o unifican en la capa de Aplicación reduciendo enormemente los costes, por esta razón es que sin lugar a dudas será una realidad en breve para todas las Operadoras del Grupo Telefónica.

Como primer aspecto, la forma más eficiente de comprender IMS es analizarlo de acuerdo a su modelo de capas. IMS opera sobre cuatro planos o capas:

- Acceso
- Transporte
- Control
- Aplicación

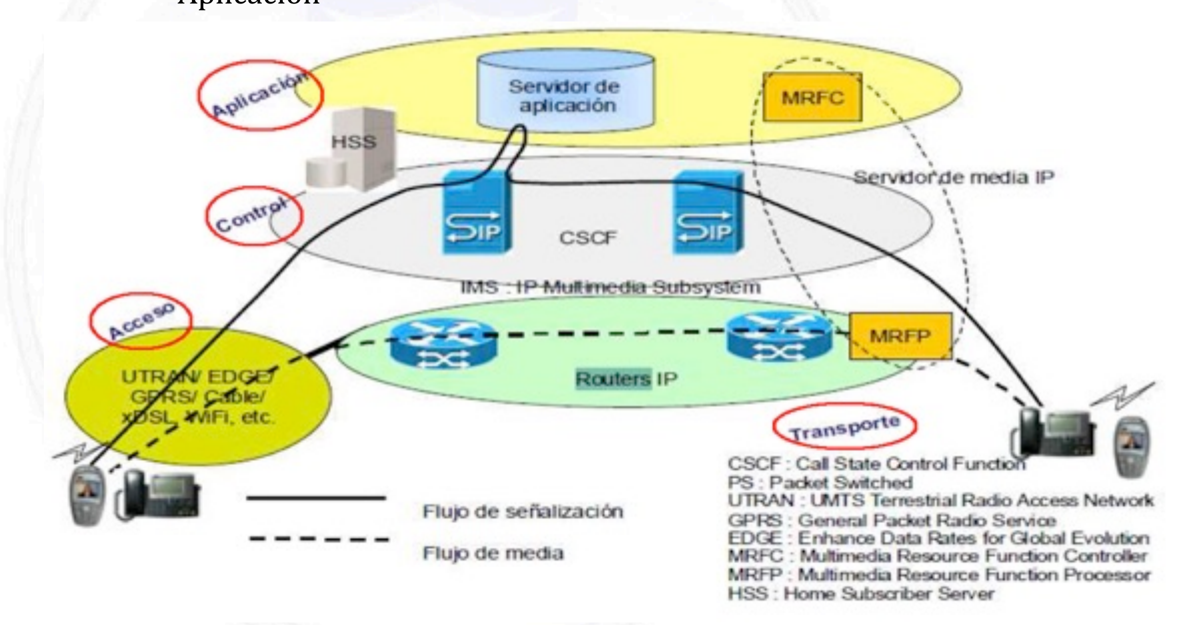


Imagen 1.22 (Planos IMS)

En la imagen anterior, se han remarcado en **“rojo”** estos planos. Como se puede apreciar, cada uno de ellos cuenta con diferentes tipos de dispositivos y funciones, a lo largo de esta sección describiremos resumidamente estos aspectos.

Capa de Acceso: Soporta cualquier tipo de acceso de alta velocidad. En nuestro caso nos centraremos en:

- Acceso Móvil
- Acceso de banda ancha Fija
- Acceso WiFi

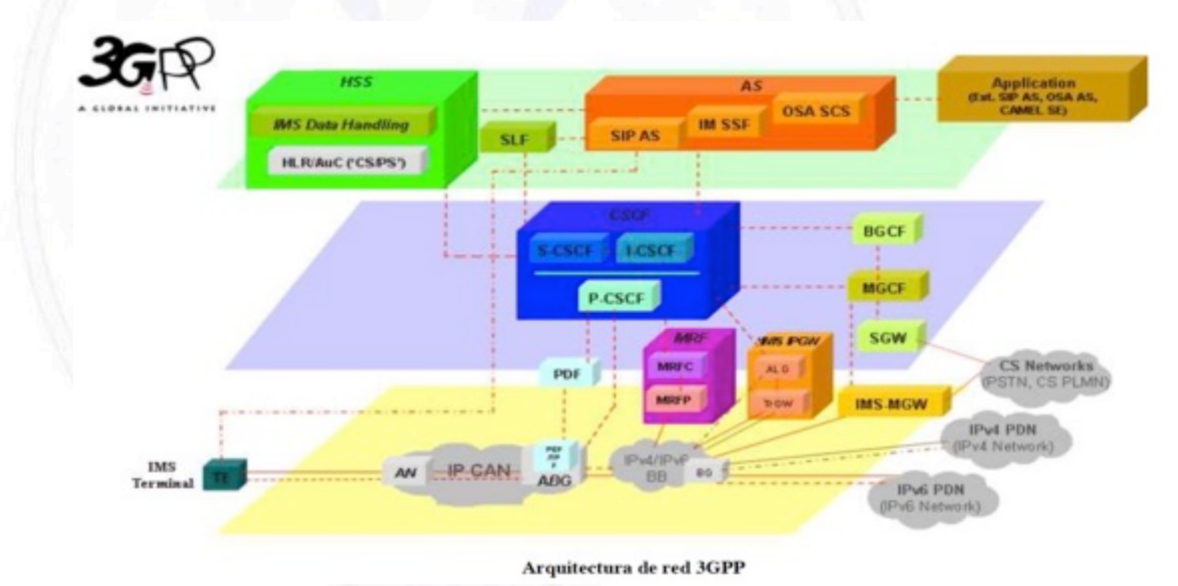
En cualquiera de estos accesos IMS soporta la conversión de protocolos, dentro de los cuales lo que más nos interesa es la conmutación de circuitos, es decir tecnologías de voz y datos que procedan de sistemas de señalización 7 (SS7) o SIGTRAN.

Capa de Transporte: Esta capa, en realidad no hace referencia la nivel 4 de modelo OSI o TCP/IP, sino que se refiere a todo el “routing IP” de cada uno de los paquetes que circulan por esta infraestructura, por lo tanto para nosotros el centro de atención de este nivel serán los routers y las reglas de filtrado que se apliquen a nivel IP y TCP/UDP.

Capa de Control: Esta es la capa central de IMS, que toma el control de la señalización y su interacción con los servidores de aplicación. Desde esta capa se lleva el control de todas las sesiones y flujos de usuarios.

Capa de Aplicación: Esta capa está conformada por los servidores de Aplicación de Media que son los responsables de integrar la totalidad de los servicios, funcionalidades y conversiones de protocolos.

A continuación haremos una breve descripción de los elementos principales de esta arquitectura. 3GPP presenta la siguiente imagen de los elementos que componen IMS:



Arquitectura de red 3GPP

Imagen 1.23 (Componentes IMS) (Imagen tomada de 3GPP)

CSCF: (Plano de Control) El CSCF (Call Session Control Function o Función de Control de Sesión de Llamada) es el elemento principal dentro de la red IMS. Es la pieza clave para la señalización a través del protocolo SIP (RFC 3261) que veremos más adelante, para establecer, modificar y terminar una sesión multimedia. Podemos pensarlo concretamente como un "Servidor SIP". Este elemento lógico desempeña tres funciones principales que pueden encontrarse en un mismo dispositivo o en hardware diferente, esta son:

- **P-CSCF**: (Proxy - Call Session Control Function) Función de control de sesión de llamada Proxy. Es el primer punto de entrada a la red IMS y actúa como entrada y salida de la misma. Toda petición iniciada desde un terminal IMS, se inicia aquí. Como veremos más adelante, es quién gestiona las peticiones SIP Registrer Request, almacenando toda la información de registro de ese "User Equipment (**UE**)". Es probable que por razones de distribución de carga, encontremos más de uno en cada Operadora.
- **I-CSCF**: (Interrogating - Call Session Control Function) Función de control de sesión de llamada. Este es el punto de contacto entre la red de la Operadora. Su principal tarea es asignar a cada usuario su correspondiente S-CSCF. Y mantener la comunicación con el **HSS** (Home Subscriber Server) empleando con este protocolo DIAMETER. En general este dispositivo es quien genera los **CDR** (Call Data Records) para la tarificación.
- **S-CSCF**: (Serving - Call Session Control Function) Función de control de sesión de servidor. Es el responsable del control y mantenimiento de las sesiones de cada UE a través del protocolo SIP, también mantiene comunicación con el HSS por medio del protocolo DIAMTER para consultas del perfil de usuario. Otra actividad importante del S-CSCF es la de consultas hacia DNS/ENUM para resolución de direccionamiento y nombres.

A su vez el CSCF ofrece otras funcionalidades que también se llevan a cabo desde el mismo dispositivo, estas son:

- Servicio de Emergencia, **E-CSCF** (Emergency CSCF), permite encaminar peticiones SIP relacionadas con llamadas o servicios de emergencia.
- Función de Control de Pasarela de Salida, **BGCF** (Break-out Gateway Control Function): Este nodo es el responsable de seleccionar las pasarelas adecuadas cuando la comunicación está relacionada con redes de conmutación de circuitos (**CS**: Circuit Switching), cuya denominación habitual cuando se trata de redes públicas es **PSTN** (Public Switching Telephone Networks). Por lo general este dispositivo, enruta las peticiones hacia los **MGCF** (Media Gateway Control Function).

- Función de Control de Entradas, **BCF** (Break-in Control Function), este es el dispositivo inverso al anterior, y actúa cuando un usuario de una red no IMS desea emplear los servicios de esta arquitectura.

El grupo 3GPP describe en su especificación técnica **TS23.228** los nodos P-CSCF, ICSCF, S-CFCS, E-CSCF y el BGC.

HSS (Home Subscriber Sever), es la evolución del **HLR** (Home Locator Register) de las redes 3G. Es donde se encuentra la base de datos y perfiles de todos los usuarios de IMS (independientemente de la tecnología de acceso: Fija, Móvil o Wifi. Es el responsable de la autenticación y registro de usuarios, como así también de los diferentes tipos de sesiones que puede establecer cada uno de ellos. Proporciona a su vez al I-CSCF la dirección del S-CSCF que el usuario tiene asignado. Las funciones del IMS se presentan en la siguiente imagen:

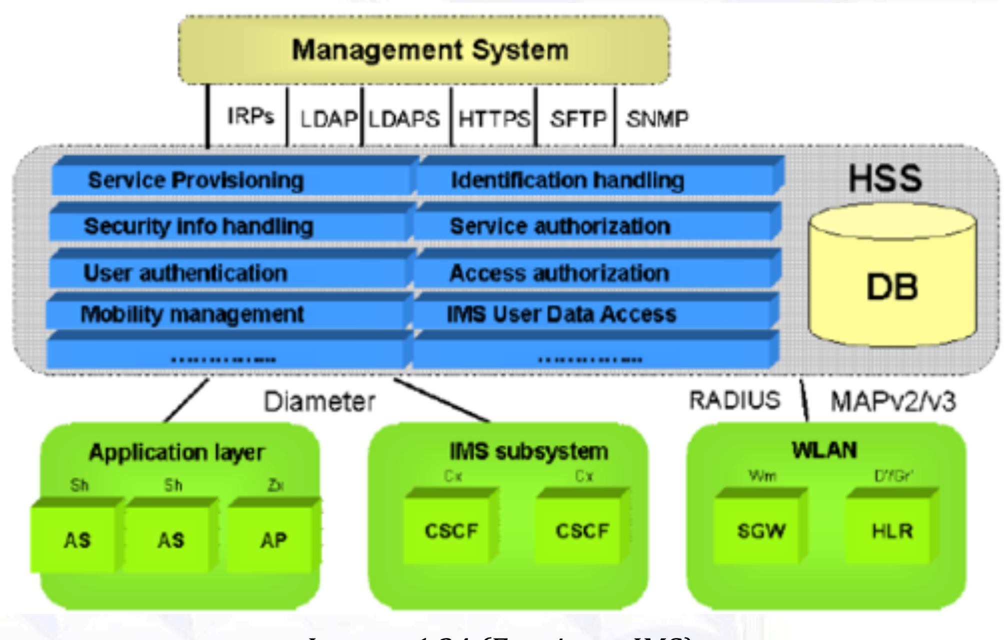


Imagen 1.24 (Funciones IMS)

SGW (Signalling Gateway): Realiza la conversión de protocolos entre ISUP/MTP o BICC/MTP a ISUP o BICC sobre SCTP/IP.

MGW (Media Gateway): Es el encargado de la comunicación en el plano de datos con la red de conmutación. Es quien envía y recibe la información del usuario a través del protocolo **RTP** (Real Time Protocol) que en realidad es por donde viaja la voz, video, etc….

MGC (Media Gateway Controller) es un sistema flexible que puede ser integrado en distintos tipos de solución, proporciona la función de señalización en la interconexión con las redes de conmutación de circuitos y de conmutación de paquetes.

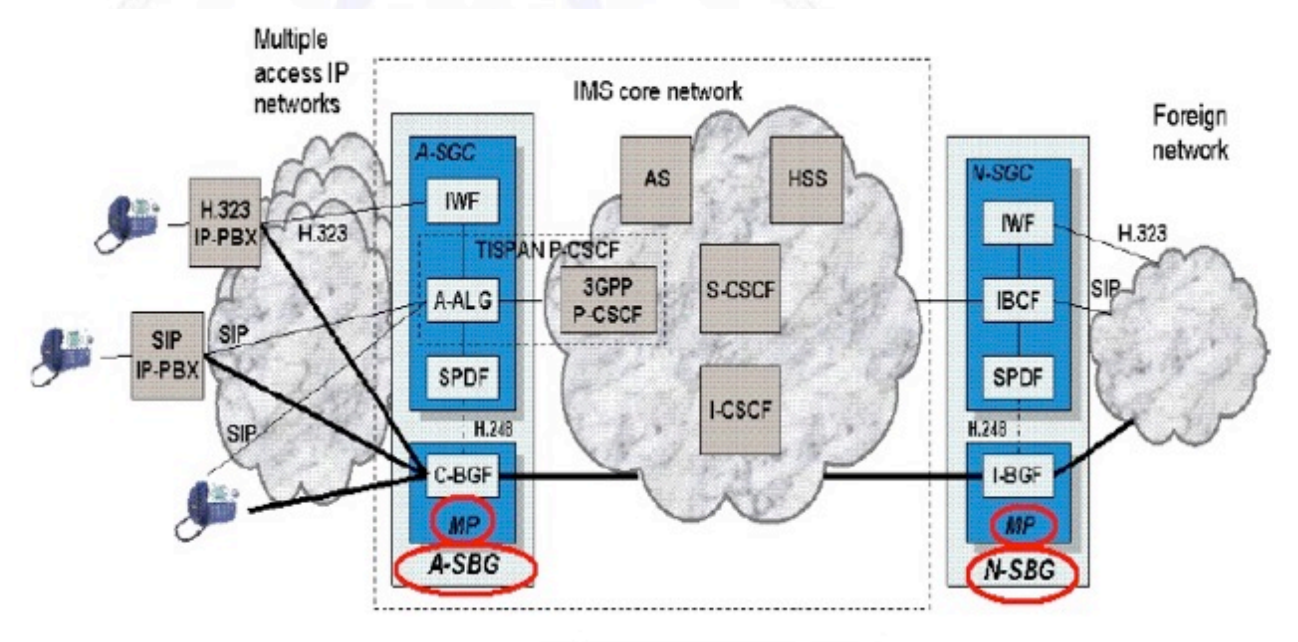
SBC (Serial o Session Border Controller) También llamado **SBG** (Gateway): es el encargado de la correlación de toda la señalización y los flujos de media (como audio y vídeo) que pasa por los extremos de la red, proporcionando un conjunto completo de funciones que son necesarias para acceder e interconectar el dominio IMS con otras redes IP multimedia. Este nodo proporciona acceso con seguridad, protección del ancho de banda, calidad del servicio, nivel de servicios acordados y otras funciones críticas para las transmisiones en tiempo real de audio o vídeo.

Desde el punto de vista de Seguridad, este debería ser uno de los principales focos de interés pues podríamos pensarlo "casi" como un Firewall de toda esta arquitectura.

El SBC se debería localizar en ambos extremos de la red, el punto de infraestructura donde una sesión pasa de una red a otra. Dentro del nodo podemos diferenciar dos partes que lo componen:

- **SGC** (Session Gateway Controller): se encarga del plano de señalización.
- **MG** (Media Gateway o también llamado **MP**: Media Proxy): soporta el tráfico de datos.

Como se muestra en la figura existen tres grandes funciones para este nodo dentro de la red:



Roles del SBC en una red IMS

Imagen 1.25 (SBC)

- **A-SGC**: cuando la funcionalidad SBG se implementa entre la red IMS core y la red de acceso. Sólo permite el tráfico de señalización hacia y desde los usuarios que están registrados en la red central IMS (en el HSS). La excepción se produciría con llamadas de emergencia de usuarios no registrados que pueden ser aceptadas si así se configura en el nodo.

- **N-SGC**: funcionalidad implementada entre la red IMS core y una red (Network) externa.

- **MP** (Media Proxy): protege los nodos centrales de la red IMS de los posibles ataques y bloquea el tráfico malicioso. Dispone de alarmas están para hacer que el operador sea consciente de posibles intentos de ataque.

Para asegurarse de que las interfaces Ethernet no se utilicen excesivamente, el MP realiza un seguimiento del ancho de banda reservado para el flujo de datos. Una parte del ancho de banda está siempre reservado para llamadas de emergencia.

Las acciones más destacables del nodo sobre la red son:

- La protección del perímetro de la red central IMS: filtrado, protección contra sobrecarga, y la limitación de velocidad para bloquear las inundaciones de tráfico IP y proporcionar protección contra la denegación de servicio (DoS).
- Registro y alertas de ataques de red y los eventos relacionados con la seguridad
- Validación de mensajes SIP / H3.23: Control de sintaxis de mensajes. Además, A-SBG sólo acepta mensajes desde los agentes de usuario registrados o mensajes de llamadas de emergencia.
- Ocultación de identidad: no hay información sobre las direcciones IP utilizadas en el núcleo de red IMS o por los usuarios de la red de acceso y la red externa.
- Permite al operador configurar el SBG funcionalidades que implementan **RTCP** (Real Time Control Protocol).
- Media anchoring: actualización de direcciones y puertos en el SDP (Session Description Protocol: parte de la familia SIP) para que los flujos pasen a través de SBG.
- asegurar la QoS: control sobre el ancho de banda disponible en cada momento.
- Permite tráfico SIP/UDP o SIP/TCP
- Soporta centralitas IP-PBX tanto SIP como H.323 y reconoce el tráfico que va desde/hacia la IP-PBX y aplica un tratamiento especial en los mensajes.

Puede modificar las cabeceras de los mensajes para direccionarlos correctamente.

- Acepta llamadas de emergencia incluso de usuarios ajenos a la red y prioriza las mismas tanto en el plano de señalización como en el de control.
- Adapta la señalización entre SIP y H.323 (N-SBG).

Un SBG puede configurarse al mismo tiempo como A-SBG y N-SBG

Como acabamos de ver este nodo es un elemento clave para la seguridad de toda Operadora.

AS (Application Servers)

Los as proporcionan la lógica de los servicios que lleve implementados IMS. Generalmente dentro de la red existen múltiples as, donde cada uno suele implementar un servicio. Los as pueden localizarse en la 'Home Network' o en redes externas, si se trata de un servicio que por ejemplo proporciona un proveedor que haya solicitado el operador de red. Todos se caracterizan por implementar Interfaz SIP hacia el S-CSCF, conocido como **ISC** (IMS Service Control). Además, estos nodos pueden implementar protocolos como HTTP o WAP necesarios para este tipo de aplicaciones.

Existen diferentes tipos de as:

- **SIP-AS**: Este as es el primero que se estableció en la red IMS, es capaz de comunicarse con el nodo HSS (basado en DIAMETER) de manera opcional si es necesario para la lógica que implementa obtener datos de este nodo. Este nodo se comunica directamente con el S-CSCF asignado al usuario de esta sesión para mantener el control SIP de la misma.

- **OSA-SCS**: (Open Service Access – Service Capability Server) con este as se permite obtener un interfaz de comunicación hacia el entorno de aplicación OSA desde la red IMS. Se conoce como Servidor de Mediación, ya que permite acceder a servicios de otra tecnología. Todos los servicios que se desarrollan hoy en día utilizan los servidores SIP, pero para las funcionalidades ya existentes en esta plataforma (OSA) se permite el acceso a través de estos as.

- **IM-SSF**: (IP Multimedia – Service Switching Function). Se trata de un servidor de mediación, que puede actuar como servidor de aplicación SIP que a la vez es capaz de comunicarse mediante el protocolo CAMEL (Customized Application for mobile-Network for Enhanced Logic) para utilizar los servicios de las redes GSM.

Media Server: Este dispositivo, no se encuentra íntegramente en la capa de Aplicación, sino que deberíamos pensarlo como en un nivel intermedio entre esta capa y la de Transporte, pues el servidor media es una plataforma utilizada para ofrecer

servicios multimedia interactivos capaces de manejar un número elevado se sesiones simultáneas en un amplio rango de configuraciones. Si volvemos a nuestra primera imagen de capas, se aprecia una unión con línea de puntos (óvalo) entre estos niveles y representa este diálogo entre ellos.

Se trata de un equipo que dispone de una funcionalidad llamada **MRF** "Multimedia Resource Function" y que provee interacciones entre usuarios y aplicaciones a través de recursos de voz y vídeo. Mediante el procesador **MRFP** "Multimedia Resource Function Controller" es posible desempeñar las funciones del tipo detección de tonalidad, síntesis y reconocimiento de voz, de traducción de media, control de recursos, envío de mensajes, grabaciones, etc.

Todo el tráfico multimedia, pasa por el MRFP si tiene que atravesar la red IMS. El tráfico entrante llega a este nodo, y es encaminado hacia su destino. También permite originar flujos de tráfico, como anuncios de audio o vídeo que envíe la propia red.

Volviendo a nuestra imagen inicial:

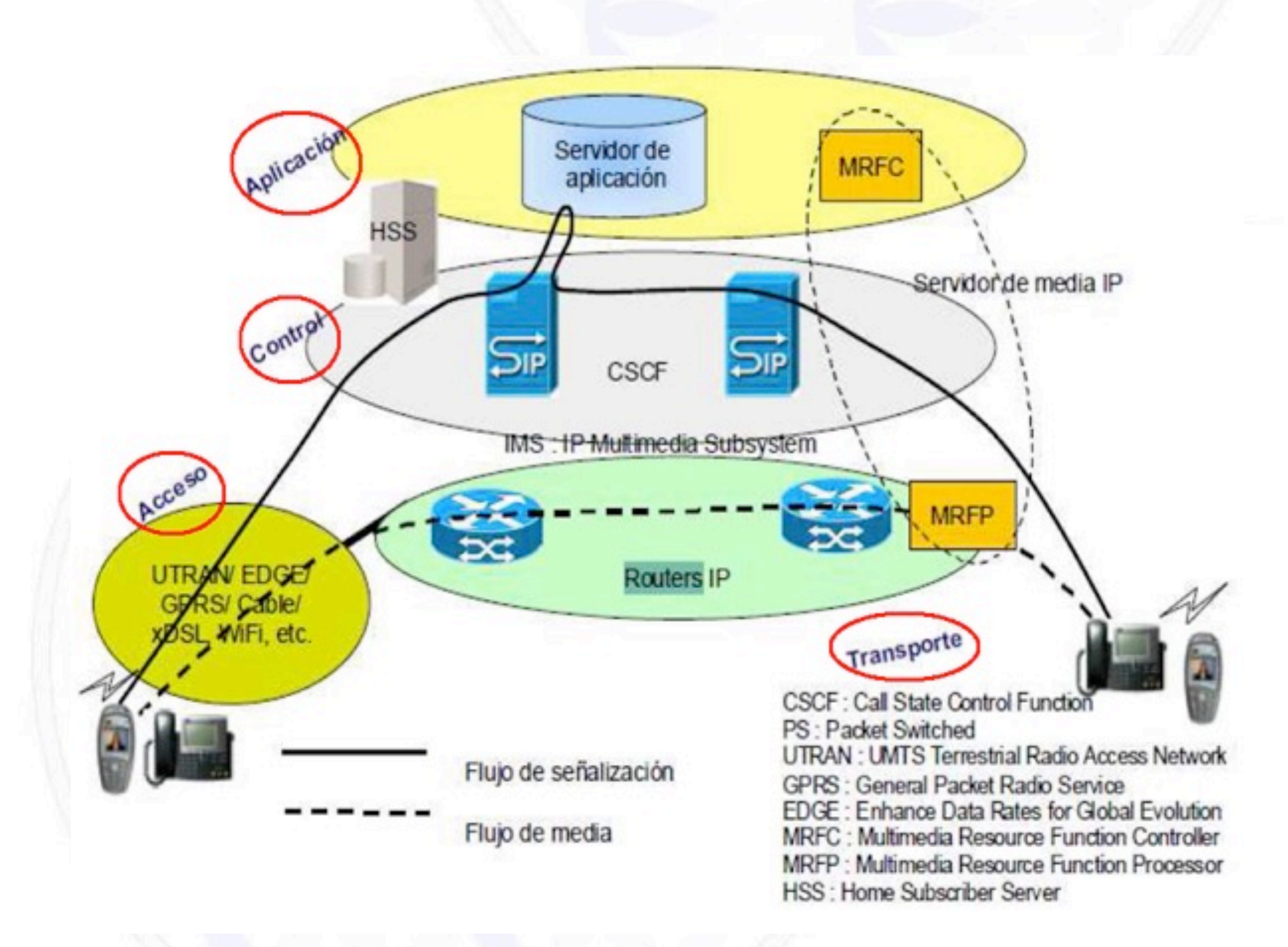


Imagen 1.26 (Planos IMS)



Ya hemos descripto los planos o capas, luego cada uno de los nodos que la componen y ahora de esta misma imagen podemos centrarnos en los dos flujos de la misma, pues son lo más importante de esta arquitectura. Podemos ver un flujo de "Media" (línea entrecortada: - - - -) que sólo circula a través de la capa de Acceso y Transporte, en definitiva por este flujo va la información de origen a destino. El otro flujo (línea continua: _____) es por donde viaja la señalización, que en IMS se trata exclusivamente del protocolo SIP, que desarrollaremos en la próxima sección. Antes de pasar a SIP, es necesario que comprendamos la siguiente imagen:

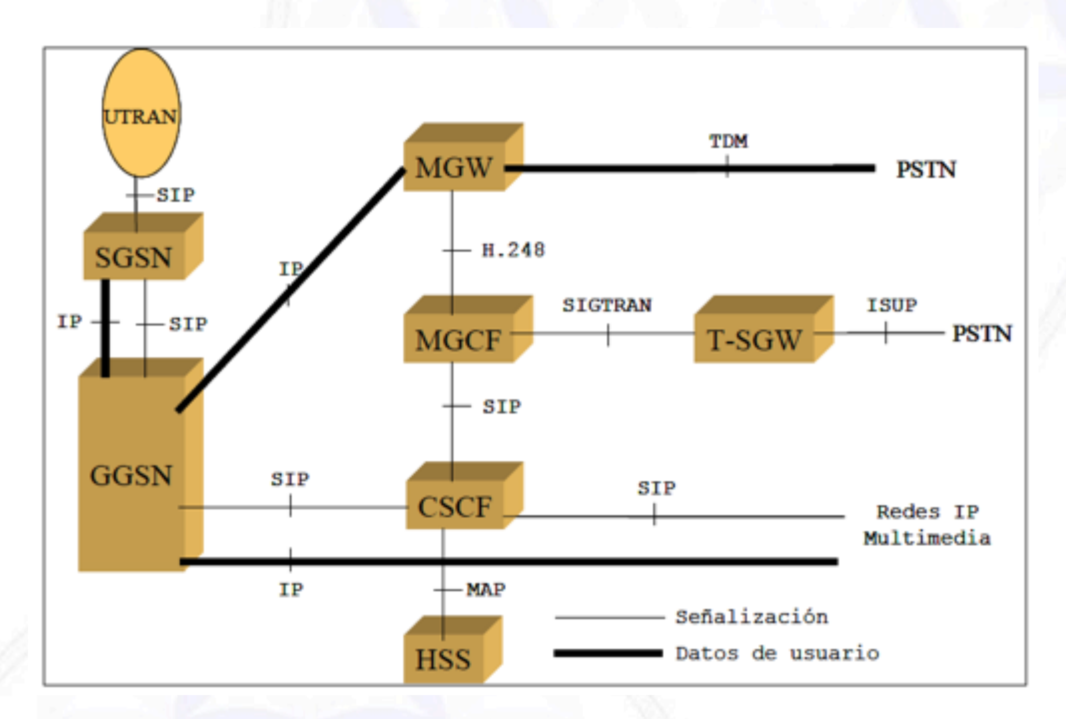


Imagen 1.27 (Salidas IMS)

En esta imagen, sólo se presenta un tipo de acceso (a la izquierda) por medio de UMTS, pero esto no es lo que deseamos destacar, sino el lado derecho de la misma, pues de este lado es donde podemos apreciar que IMS (a través de los nodos que acabamos de presentar) está en capacidad de comunicarse con redes cuya señalización presente cualquier tipo de protocolos, en este caso vemos comunicación con:

- PSTN a través de **TDM** (multiplexación por división de tiempo: SS7)
- PSTN a través de **SIGTRAN** (señalización de nivel Transporte)
- Redes IP Multimedia a través de **SIP**.

Hemos cerrado la sección con esta imagen para remarcar el rol de cada uno de los dispositivos que operan sobre estos intercambios de señalización.

1.8. SIP (Session Initiation Protocol)

La inmensa mayoría de los artículos sobre **SIP** están relacionados con **VoIP** (Voice over IP), pero esto es solo la punta de iceberg, **lo verdaderamente importante de este protocolo es su inminente implantación en las redes de 4G** que es lo que se presenta en esta sección.

Tal cual hemos estado viendo, la evolución de las redes de voz (fija, móvil y hoy de datos) nos lleva a un camino sin salida hacia **SIP** (Session Initiation Protocol). Lo más importante es que se trata de un protocolo de **señalización** que reemplazará el **SS7** (Sistema de señalización 7, con 35 años de vida….). Quien controle este sistema, dominará las entrañas de una red de telecomunicaciones de extremo a extremo. En los últimos 15 años, se han publicado más de 160 **RFC**s (Request for Comments) desarrollando este protocolo (*es prácticamente un caso único*). La integración de voz y datos se llama **LTE** o **4G**, su concepto rector es "**all IP**" bajo la arquitectura que acabamos de ver llamada **IMS** (Internet Multimedia Subystem) y todo ello sustentado por la señalización **SIP**…… ya existen un sinnúmero de debilidades presentadas en referencia a SIP…. Si lo conociéramos más en detalle la "seguridad" de las futuras redes IP estaría en nuestras manos (*para bien o para mal*).

Toda esta sección se basa, e intenta transmitir, la experiencia obtenida en el trabajo de seguridad en redes en operadoras de telefonía (fija y móvil, actualmente redes de voz y datos) en gran parte de Europa y todo Sudamérica, actividad en la que se conoce en detalle la trascendencia de la señalización y cómo toda esta infraestructura de telecomunicaciones dependerá absolutamente de **SIP**, por esta razón es que se considera de vital importancia comenzar a despertar el interés sobre la investigación de la seguridad de este protocolo (*objetivo primario de estos párrafos*), más allá del mero concepto de VoIP.

1.8.1. Señalización.

Iniciemos nuestra presentación de SIP recordando algunos conceptos básicos de este tema. La señalización es el conjunto de medidas que se acuerdan para:

- Establecimiento
- Mantenimiento
- Cierre de la comunicación

Tipos:

- En banda
- Fuera de banda
- Canal común
- Canal independiente (canal asociado)

Tomemos como referente importante al **SS7** que comienza a ser desarrollado en 1975, definido como estándar en 1981 (reemplazando a SS5, SS6 y R2).

SS5 y anteriores eran señalización dentro de banda. SS7 es fuera de banda por canal común (Pues separa la señalización de los canales portadores). Podemos mencionar aquí dos metodologías:

- **CAS** (Channel Associated Signalling) o señalización por canal asociado: Los datos/voz viajan por el mismo/igual camino.
- **CCS** (Common Channel Signalling) o señalización por canal común: Datos/voz y señalización viajan por caminos diferentes. En un solo canal de señalización se lleva la información de varios canales de voz/datos.

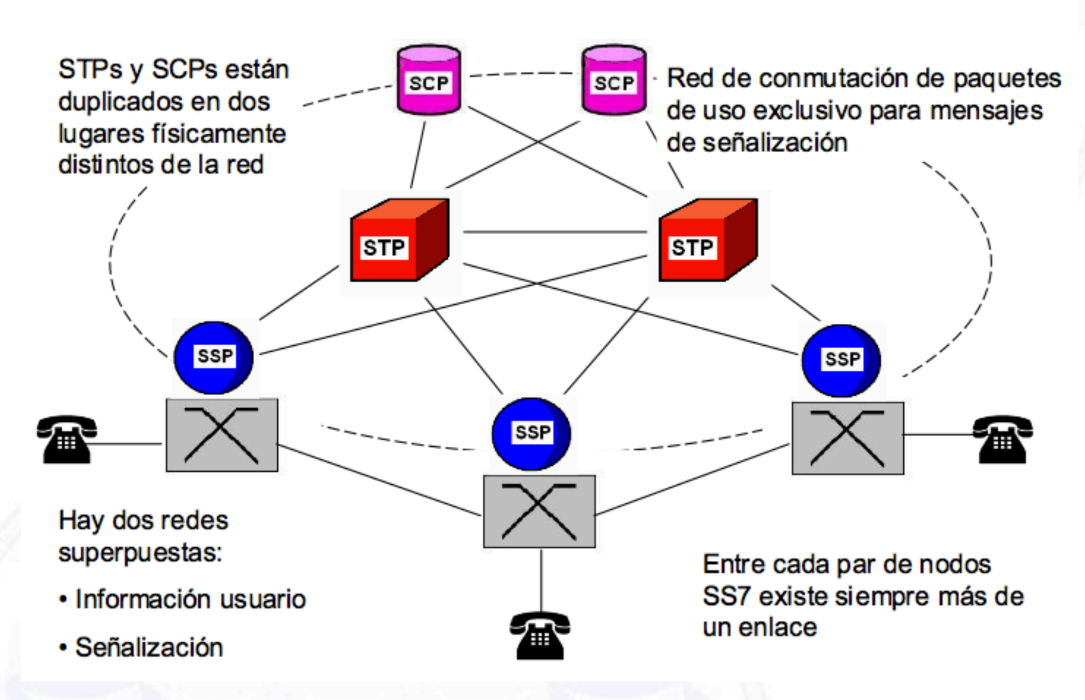


Imagen 1.28 *(Estructura de una red SS7 – **SCP**=Service Control Point, **SSP**=Service Switching Point, **STP**= Signal Transfer Point)*

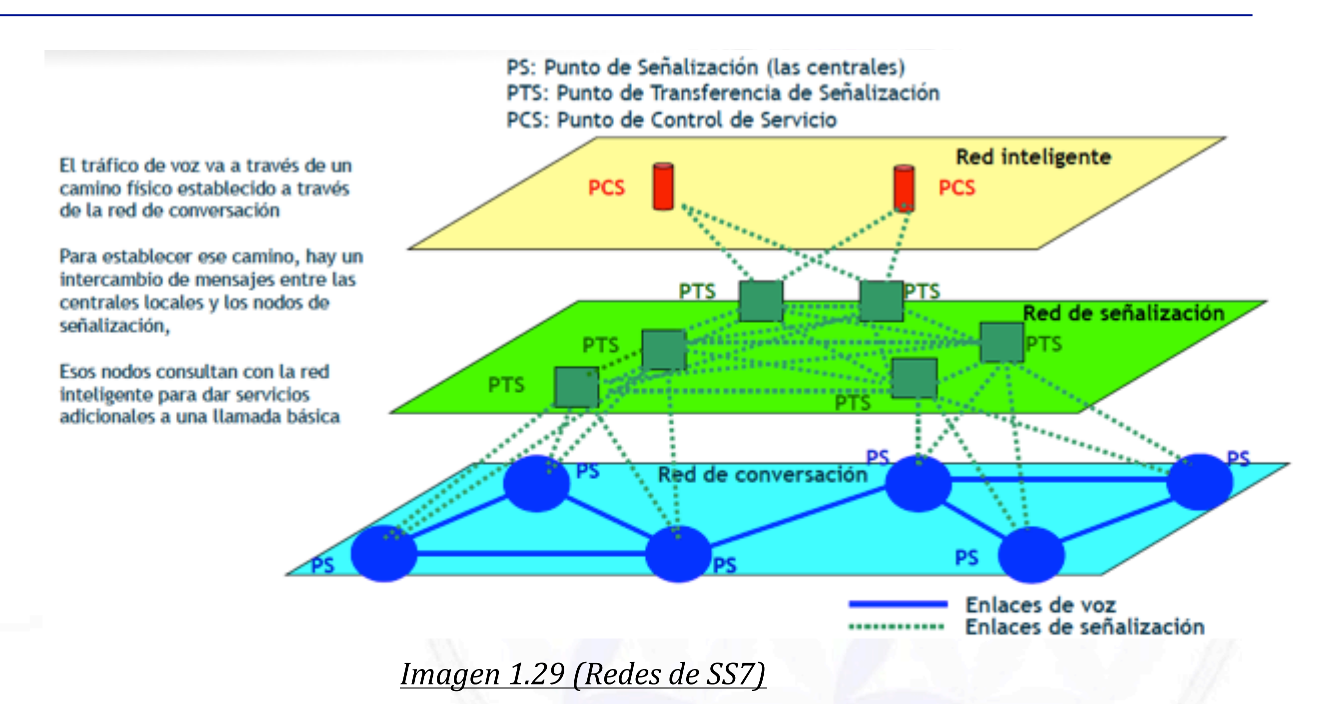


Imagen 1.29 (Redes de SS7)

El segundo hito importante para nosotros en la historia de la señalización, es el que estuvimos viviendo con **SIGTRAN** o (Señalización de Transporte).

> Apreciación estrictamente personal: Hoy el mundo no puede plantearse la comunicación de extremo a extremo como "Conmutación de **paquetes**" ya necesita poder conmutar "**Flujos**" de datos (o de contenidos).

SIGTRAN, como hemos visto, no deja de ser una solución de compromiso hacia lo que se nos viene encima cuando el mundo sea "all IP", y es aquí donde entra en juego **SIP**.

Lo que las Telco están lanzando a través de **LTE** (o **4G**) es **IMS**...... y el mundo será "**all IP**".

La señalización de IMS es **SIP**.

Lo primero que se debe destacar es que el concepto de la sección anterior de **IMS**, si deseamos resumirlo es la evolución de NGN con el empleo del protocolo "**SIP**" para señalización. (esta sería la idea fuerza, un subsistema de señalización).

La segunda idea fuerza debería ser que como todo este subsistema requiere direccionamiento IP, lo más natural es pensarlo con visión "**IP versión 6**", pues la actual versión 4 no soportará tanto direccionamiento (o implicará un gran esfuerzo de **NAT**: Network Access Translation).

NOTA: Si se desea ampliar sobre la familia de protocolos IP versión 6, pueden descargarse en forma gratuita los siguientes artículos desde la página inicial de la web de **DarFe** (http://www.darFe.es):

- **"IPv6 (Parte_01) - Componentes"**
- **"IPv6 (Parte_02) - Direcciones"**
- **"IPv6 (Parte_03) - Encabezado"**

El control de sesión es realizado por el protocolo de control de llamada basado en SIP (Session Initiation Protocol) y **SDP** (Session Description Protocol). SIP aporta funciones para el registro, establecimiento, liberación y mantenimiento de las sesiones IMS, también habilita todo tipo de servicios suplementarios. El protocolo SIP tiene una estructura similar a HTTP y comparte los códigos de respuesta facilitando el desarrollo de los servicios, puesto que es similar a construir aplicaciones web. Tanto SIP como HTTP son protocolos de texto, que permiten incluir contenido MIME en el cuerpo de sus mensajes. El protocolo **SDP**, se emplea para describir la sesión que se negocia con SIP. Mediante SDP, los extremos de una sesión pueden indicar sus capacidades multimedia y definir el tipo de sesión que se desea mantener. Mediante este intercambio de señalización se negocia la QoS, tanto en el establecimiento como durante la sesión en curso, si es necesario.

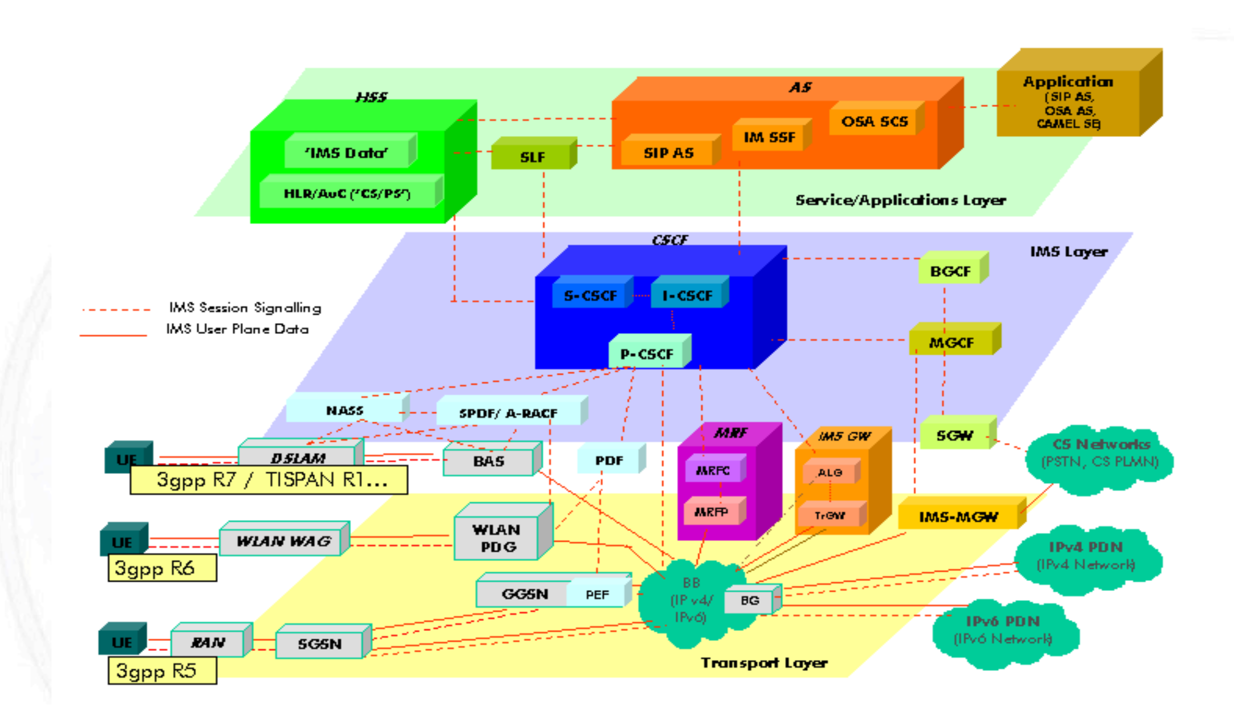


Imagen 1.30 (Niveles) tomada de Wikipedia



Imagen1.31 (Servicios) tomada de la presentación de ZTE sobre IMS

Además de SIP/SDP e IPv6, 3GPP emplea otros protocolos de IETF para la provisión de servicios IP multimedia, como son:

- Los protocolos **RTP** (Real Time Protocol) y RTCP (Real Time Control Protocol), que se utilizan para el transporte de flujos IP multimedia del plano de usuario.
- El protocolo **COPS** (Common Open Policy Service), para el control de los recursos de GPRS mediante el uso de políticas de asignación de los mismos en función de los objetivos marcados de calidad.
- El protocolo **Diameter**, para aquellas acciones relacionadas con la autorización, autenticación y tarificación. Principalmente se emplea como heredero de MAP para el diálogo con el nodo HSS (Home Subscriber Server) de IMS, que sustituye las funciones realizadas por el tradicional HLR (Home Location Register).
- Los protocolos **RSVP** (Resource Reservation Protocol) y DiffServ, para asegurar la QoS extremo a extremo, especialmente cuando la conectividad IP requerida se extiende más allá de la red móvil GPRS.
- El protocolo **Megaco**, para el control remoto de los Media Gateways.

Se pueden descargar varias capturas de estos protocolos en www.darFe.es

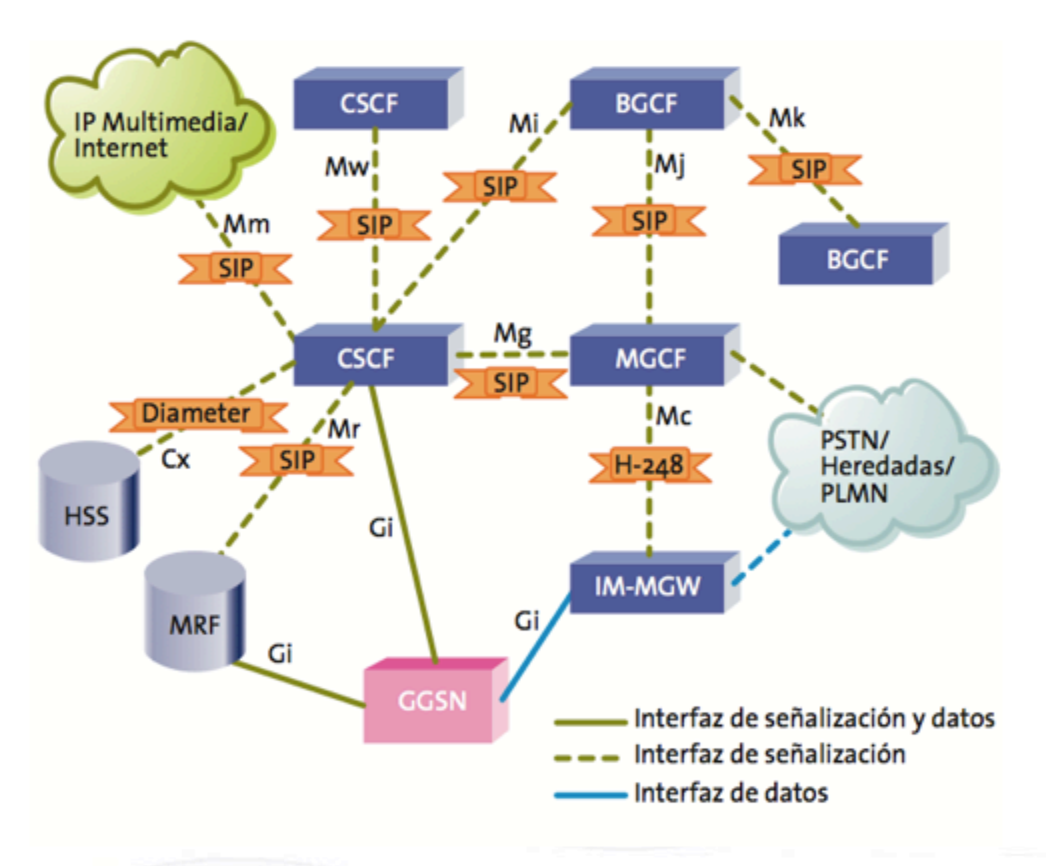


Imagen 1.32 (Arquitectura de IMS)

1.8.2. La entrada en escena de SIP.

En primer lugar deseo poner de manifiesto las RFCs que tratan este protocolo, pues es llamativo la cantidad que posee (*lo cual demuestra la importancia que se le está dando*):

2543 SIP: Session Initiation Protocol.
2848 The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services.
3261 SIP: Session Initiation Protocol (Obsoletes: 2543).
3262 Reliability of Provisional Responses in Session Initiation Protocol (SIP).
3263 Session Initiation Protocol (SIP): Locating SIP Servers.
3264 An Offer/Answer Model with Session Description Protocol (SDP).
3265 Session Initiation Protocol (SIP)-Specific Event Notification.
3266 Support for IPv6 in Session Description Protocol (SDP).
3267 Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs.
3311 The Session Initiation Protocol (SIP) UPDATE Method.
3312 Integration of Resource Management and Session Initiation Protocol (SIP).
3313 Private Session Initiation Protocol (SIP) Extensions for Media Authorization.
3319 Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers.

3325 Private Extensions to the Session Initiation Protocol (SIP) for asserted Identity within Trusted Networks.
3326 The Reason Header Field for the Session Initiation Protocol (SIP).
3327 Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts.
3329 Security Mechanism Agreement for the Session Initiation Protocol (SIP).
3351 User Requirements for the Session Initiation Protocol (SIP) in Support of Deaf, Hard of Hearing and Speech-impaired Individuals.
3361 Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers.
3372 Session Initiation Protocol for Telephones (SIP-T): Context and Architectures.
3427 Change Process for the Session Initiation Protocol (SIP).
3428 Session Initiation Protocol (SIP) Extension for Instant Messaging.
3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP)
3485 The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp).
3486 Compressing the Session Initiation Protocol (SIP).
3487 Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP).
3515 The Session Initiation Protocol (SIP) Refer Method.
3665 Session Initiation Protocol (SIP) Basic Call Flow Examples.
3666 Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows.
3680 A Session Initiation Protocol (SIP) Event Package for Registrations.
3702 Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP).
3764 enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record.
3824 Using E.164 numbers with the Session Initiation Protocol (SIP).
3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP).
3841 Caller Preferences for the Session Initiation Protocol (SIP).
3842 A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP).
3853 S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP).
3856 A Presence Event Package for the Session Initiation Protocol (SIP).
3857 A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP).
3891 The Session Initiation Protocol (SIP) "Replaces" Header.
3892 The Session Initiation Protocol (SIP) Referred-By Mechanism.
3893 Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format.
3903 Session Initiation Protocol (SIP) Extension for Event State Publication.
3911 The Session Initiation Protocol (SIP) "Join" Header.
3959 The Early Session Disposition Type for the Session Initiation Protocol (SIP).
3960 Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP).
3968 The Internet assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol.
3969 The Internet assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP).
3976 Interworking SIP and Intelligent Network (IN) Applications.
4028 Session Timers in the Session Initiation Protocol (SIP).
4032 Update to the Session Initiation Protocol (SIP) Preconditions Framework.
4083 Input 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP).
4092 Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP).
4117 Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc).
4123 Session Initiation Protocol (SIP)-H.323 Interworking Requirements.
4168 The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP).

4189 Requirements for End-to-Middle Security for the Session Initiation Protocol (SIP).
4235 An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP).
4240 Basic Network Media Services with SIP.
4244 An Extension to the Session Initiation Protocol (SIP) for Request History Information.
4245 High-Level Requirements for Tightly Coupled SIP Conferencing.
4320 Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction.
4321 Problems Identified associated with the Session Initiation Protocol's (SIP) Non-INVITE Transaction.
4353 A Framework for Conferencing with the Session Initiation Protocol (SIP).
4354 A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service.
4411 Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events.
4412 Communications Resource Priority for the Session Initiation Protocol (SIP).
4453 Requirements for Consent-Based Communications in the Session Initiation Protocol (SIP).
4457 The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-Header).
4458 Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR).
4474 Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP).
4475 Session Initiation Protocol (SIP) Torture Test Messages.
4483 A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages.
4484 Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP).
4485 Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP).
4488 Suppression of Session Initiation Protocol (SIP) REFas Method Implicit Subscription.
4497 Interworking between the Session Initiation Protocol (SIP) and QSIG.
4504 SIP Telephony Device Requirements and Configuration.
4508 Conveying Feature Tags with the Session Initiation Protocol (SIP) REFas Method.
4538 Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP).
4575 A Session Initiation Protocol (SIP) Event Package for Conference State.
4579 Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents.
4596 Guidelines for Usage of the Session Initiation Protocol (SIP) Caller Preferences Extension.
4662 A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists.
4730 A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML).
4740 Diameter Session Initiation Protocol (SIP) Application.
4780 Management Information Base for the Session Initiation Protocol (SIP).
4916 Connected Identity in the Session Initiation Protocol (SIP).
5002 The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header).
5009 Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media.
5039 The Session Initiation Protocol (SIP) and Spam.
5049 Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP).
5079 Rejecting Anonymous Requests in the Session Initiation Protocol (SIP).
5118 Session Initiation Protocol (SIP) Torture Test Messages for Internet Protocol Version 6 (IPv6).
5194 Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP).
5196 Session Initiation Protocol (SIP) User Agent Capability Extension to Presence Information Data Format (PIDF).
5263 Session Initiation Protocol (SIP) Extension for Partial Notification of Presence Information.
5318 The Session Initiation Protocol (SIP) P-Refused-URI-List Private-Header (P-Header).
5360 A Framework for Consent-Based Communications in the Session Initiation Protocol (SIP).
5362 The Session Initiation Protocol (SIP) Pending Additions Event Package.
5363 Framework and Security Considerations for Session Initiation Protocol (SIP) URI-List Services.
5365 Multiple-Recipient MESSAGE Requests in the Session Initiation Protocol (SIP).
5366 Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP).
5367 Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP).
5368 Referring to Multiple Resources in the Session Initiation Protocol (SIP).

5369 Framework for Transcoding with the Session Initiation Protocol (SIP).
5370 The Session Initiation Protocol (SIP) Conference Bridge Transcoding Model.
5373 Requesting Answering Modes for the Session Initiation Protocol (SIP).
5379 Guidelines for Using the Privacy Mechanism for SIP.
5393 Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies.
5407 Example Call Flows of Race Conditions in the Session Initiation Protocol (SIP).
5411 A Hitchhiker's Guide to the Session Initiation Protocol (SIP).
5478 IANA Registration of New Session Initiation Protocol (SIP) Resource-Priority Namespaces.
5502 The SIP P-Served-User Private-Header (P-Header) for the 3GPP IP Multimedia (IM) Core Network (CN) Subsystem.
5503 Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture.
5509 Internet assigned Numbers Authority (IANA) Registration of Instant Messaging and Presence DNS SRV RRs for the Session Initiation Protocol (SIP).
5552 SIP Interface to VoiceXML Media Services.
5589 Session Initiation Protocol (SIP) Call Control - Transfer.
5606 Implications of 'retransmission-allowed' for SIP Location Conveyance.
5621 Message Body Handling in the Session Initiation Protocol (SIP).
5626 Managing Client-Initiated Connections in the Session Initiation Protocol (SIP).
5627 Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP).
5628 Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routable User Agent URIs (GRUUs).
5629 A Framework for Application Interaction in the Session Initiation Protocol (SIP).
5630 The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP).
5631 Session Initiation Protocol (SIP) Session Mobility.
5638 Simple SIP Usage Scenario for Applications in the Endpoints.
5658 Addressing Record-Route Issues in the Session Initiation Protocol (SIP).
5688 A Session Initiation Protocol (SIP) Media Feature Tag for MIME Application Subtypes.
5727 Change Process for the Session Initiation Protocol (SIP) and the Real-time Applications and Infrastructure Area.
5767 User-Agent-Driven Privacy Mechanism for SIP.
5768 Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP).
5806 Diversion Indication in SIP.
5839 An Extension to Session Initiation Protocol (SIP) Events for Conditional Event Notification.
5850 A Call Control and Multi-Party Usage Framework for the Session Initiation Protocol (SIP).
5853 Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments.
5876 Updates to asserted Identity in the Session Initiation Protocol (SIP).
5897 Identification of Communications Services in the Session Initiation Protocol (SIP).
5898 Connectivity Preconditions for Session Description Protocol (SDP) Media Streams.
5922 Domain Certificates in the Session Initiation Protocol (SIP).
5923 Connection Reuse in the Session Initiation Protocol (SIP).
5924 Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates.
5947 Requirements for Multiple Address of Record (AOR) Reachability Information in the Session Initiation Protocol (SIP).
5989 A SIP Event Package for Subscribing to Changes to an HTTP Resource.
6011 Session Initiation Protocol (SIP) User Agent Configuration.
6026 Correct Transaction Handling for 2xx Responses to Session Initiation Protocol (SIP) INVITE Requests.
6044 Mapping and Interworking of Diversion Information between Diversion and History-Info Headers in the Session Initiation Protocol (SIP).
6045 Real-time Inter-network Defense (RID).
6046 Transport of Real-time Inter-network Defense (RID) Messages.
6050 A Session Initiation Protocol (SIP) Extension for the Identification of Services.

6072 Certificate Management Service for the Session Initiation Protocol (SIP).
6076 Basic Telephony SIP End-to-End Performance Metrics.
6086 Session Initiation Protocol (SIP) INFO Method and Package Framework.
140 Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP).
6141 Re-INVITE and Target-Refresh Request Handling in the Session Initiation Protocol (SIP).
6157 IPv6 Transition in the Session Initiation Protocol (SIP).
6216 Example Call Flows Using Session Initiation Protocol (SIP) Security Mechanisms.
6228 Session Initiation Protocol (SIP) Response Code for Indication of Terminated Dialog.
6271 Requirements for SIP-Based Session Peering.
6314 NAT Traversal Practices for Client-Server SIP.
6337 Session Initiation Protocol (SIP) Usage of the Offer/Answer Model.
6341 Use Cases and Requirements for SIP-Based Media Recording (SIPREC).
6342 Mobile Networks Considerations for IPv6 Deployment.
6357 Design Considerations for Session Initiation Protocol (SIP) Overload Control.
6405 Voice over IP (VoIP) SIP Peering Use Cases.
6432 Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses.
6446 Session Initiation Protocol (SIP) Event Notification Extension for Notification Rate Control.
6447 Filtering Location Notifications in the Session Initiation Protocol (SIP).
6461 Data for Reachability of Inter-/Intra-NetworK SIP (DRINKS) Use Cases and Protocol Requirements.
6468 Sieve Notification Mechanism: SIP MESSAGE.
6567 Problem Statement and Requirements for Transporting User-to-User Call Control Information in SIP.
6665 SIP-Specific Event Notification.
6794 A Framework for Session Initiation Protocol (SIP) Session Policies.
6795 A Session Initiation Protocol (SIP) Event Package for Session-Specific Policies.
6809 Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP).
6872 The Common Log Format (CLF) for the Session Initiation Protocol (SIP): Framework and Information Model.
6873 Format for the Session Initiation Protocol (SIP) Common Log Format (CLF).
6878 IANA Registry for the Session Initiation Protocol (SIP) "Priority" Header Field.
6910 Completion of Calls for the Session Initiation Protocol (SIP).
6913 Indicating Fax over IP Capability in the Session Initiation Protocol (SIP).
6914 SIMPLE Made Simple: An Overview of the IETF Specifications for Instant Messaging and Presence Using (SIP).
6993 Instant Messaging and Presence Purpose for the Call-Info Header Field in the Session Initiation Protocol (SIP).
7044 An Extension to the Session Initiation Protocol (SIP) for Request History Information.
7081 CUSAX: Combined Use of the Session Initiation Protocol and the Extensible Messaging and Presence Protocol (XMPP).
7092 A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents.
7106 A Group Text Chat Purpose for Conference and Service URIs in the SIP Event Package for Conference State.
7118 The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP).
7131 Session Initiation Protocol (SIP) History-Info Header Call Flow Examples.
7135 Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications.
7200 A Session Initiation Protocol (SIP) Load-Control Event Package.
7201 Options for Securing RTP Sessions.
7202 Securing the RTP Framework: Why RTP Does Not Mandate a Single Media Security Solution.
7247 Interworking between the Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP): Architecture, Addresses, and Error Handling.
7248 Interworking between the Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP): Presence.
7315 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP.

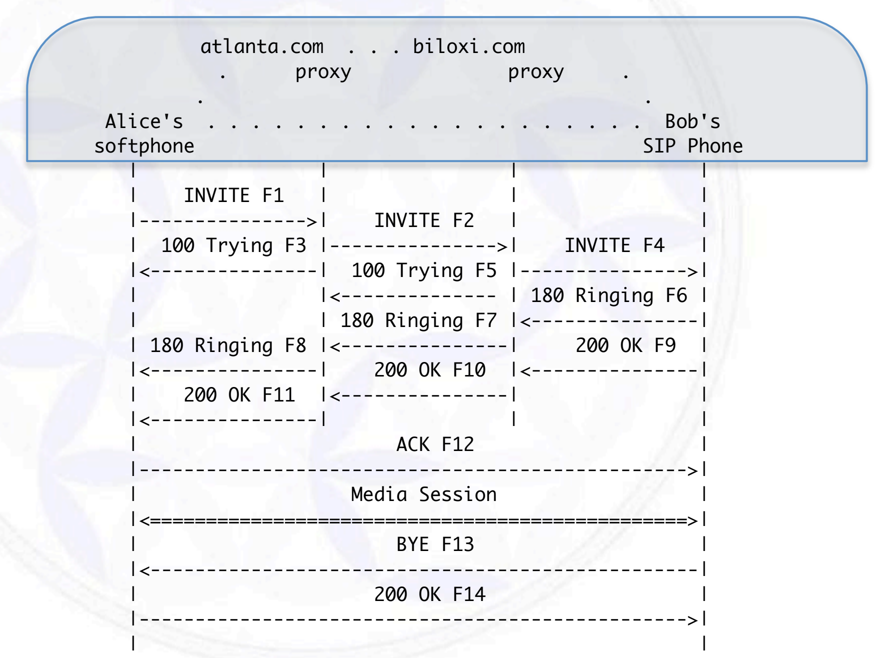


7316 The Session Initiation Protocol (SIP) P-Private-Network-Indication Private Header (P-Header).
7329 A Session Identifier for the Session Initiation Protocol (SIP).
7332 Loop Detection Mechanisms for Session Initiation Protocol (SIP) Back-to-Back User Agents (B2BUas).
7339 Session Initiation Protocol (SIP) Overload Control.
7355 Indicating WebSocket Protocol as a Transport in the Session Initiation Protocol (SIP) Common Log Format (CLF).
7403 A Media-Based Traceroute Function for the Session Initiation Protocol (SIP).

Cada una de las RFCs presentadas describen aspectos a considerar en el empleo de SIP, el cual no difiere en su lógica de http en cuanto al mecanismo y formato de sus mensajes, ofreciendo muchas alternativas para configurar su autenticación, confidencialidad e integridad características sobre las que llama la atención la poca importancia que se está dando en redes reales de operadoras telefónicas que ya están en producción.

De las RFC presentadas, nos centraremos en la **RFC-3261** (*SIP: Session Initiation Protocol*) esta es el mayor referente a la hora de analizar SIP.

Lo primero que debemos considerar es que SIP sólo es responsable de la **SEÑALIZACIÓN** *(considerando también el protocolo SDP Session Description Protocol **RFC-2327** que forma parte de esta actividad*). Los flujos de datos viajan concretamente por otra "Portadora" como veremos más adelante. Por esta razón es que la comunicación de VoIP (o en nuestro caso VoLTE) se define como "Trapezoidal", tal cual podemos ver en la figura que presentamos a continuación (que es textualmente como la presenta la RFC-3261):



RFC 3261-SIP - Figure1: SIP session setup example with SIP trapezoid

Lo que se acaba de presentar en la imagen anterior, es este doble flujo que se presenta en las comunicaciones de VoIP:

- Un flujo de señalización (SIP/SDP).
- Un flujo de datos (en nuestro caso RTP/RTCP).

Independientemente de toda la información que se puede encontrar en Internet acerca de VoIP, para nuestro análisis, nos vamos a centrar en los conceptos que ya hemos visto de **VoLTE** y específicamente en lo que sucede dentro de las arquitecturas de las operadoras de telefonía internacionales *(es decir específicamente en los despliegues de VolTE*). Para un despliegue de VoLTE, como ya hemos presentado, es necesario contar con dos tecnologías:

- **LTE** (Long Term Evolution)
- **IMS** (IP Multimedia Subsystem)

En las operadoras telefónicas, podríamos plantear el despliegue de las redes móviles, tal cual se presenta a continuación.

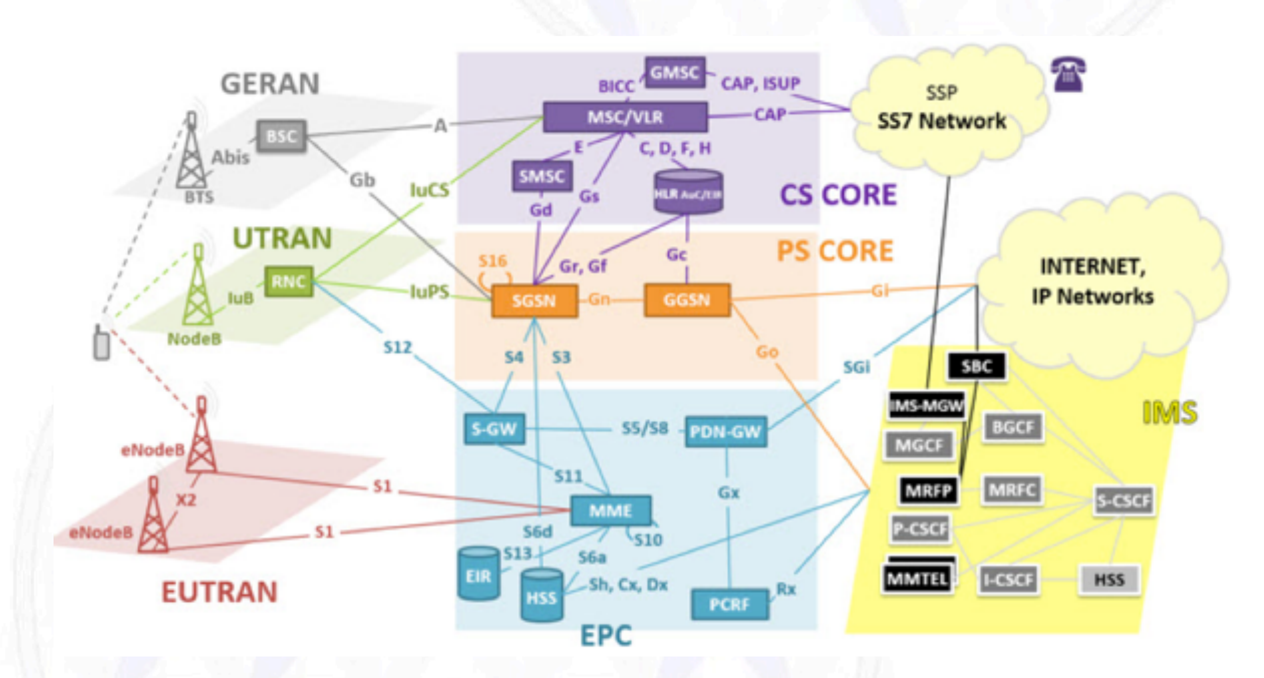


Imagen 1.33 (Despliegues de difernetes generaciones móviles)

En la imagen anterior vemos las arquitecturas de 2G, 3G y 4G, en la última de ellas, y a la derecha, se presenta un esquema típico de IMS.

Básicamente, la conexión de un Mobile Equipment (**ME**) a una red VoLTE dependerá fundamentalmente de que la red pueda ofrecerle la calidad de servicio necesaria. Para que esto se cumpla (y lo podamos entender) recordemos nuevamente los conceptos de identificador de clase de QoS (**QCI**) la Plantilla de Flujo de Tráfico

(**TFT**: Traffic Flow Template) Desarrollados en el punto 1.5. Voz sobre IP y VoLTE. Lo que estábamos diciendo en esos párrafos es que en una infraestructura LTE, cuando se implanta VoLTE existirán dos "flujos" diferentes:

- Uno de señalización
- Otro de datos

PRIMERA REFLEXIÓN DE SEGURIDAD: Al analizar la seguridad de SIP, debemos tener claro que tiene **una portadora exclusiva** y con su propia IP para este tráfico que no debemos confundir con los caminos de datos o voz.

Se presenta a continuación un sencillo esquema de estos dos flujos.

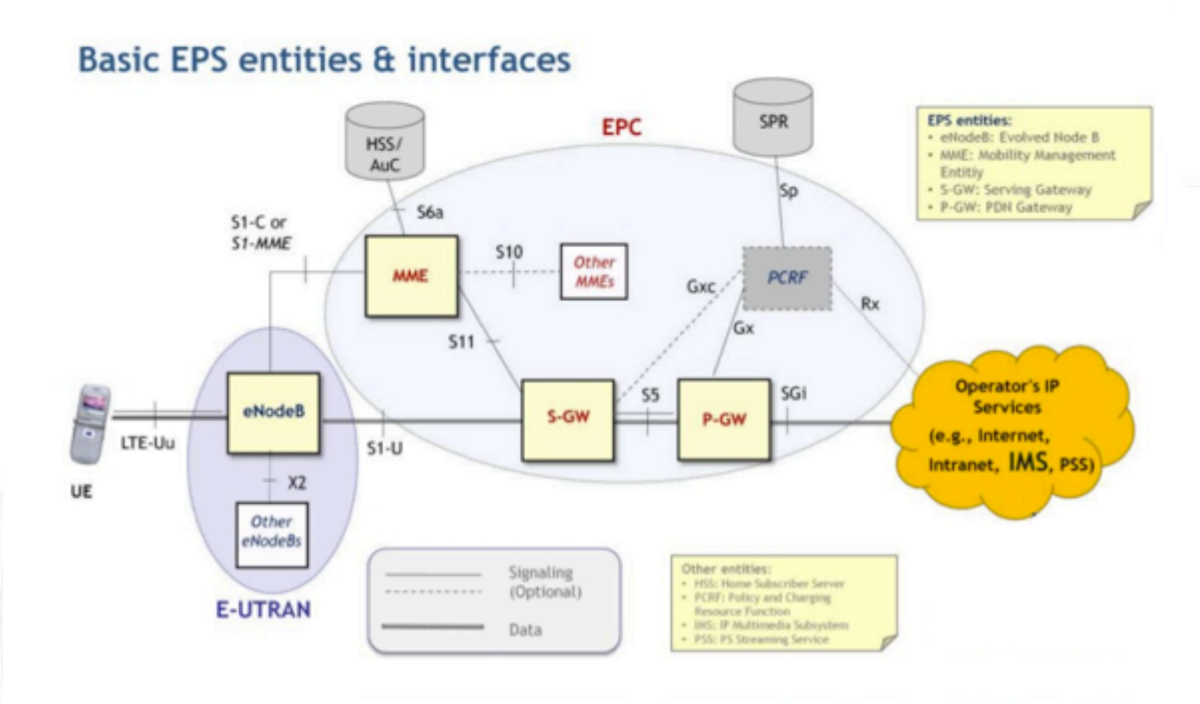


Imagen 1.34 (Arquitectura LTE)

Si entramos más en detalle sobre estos dos flujos, podemos analizar la figura que sigue.

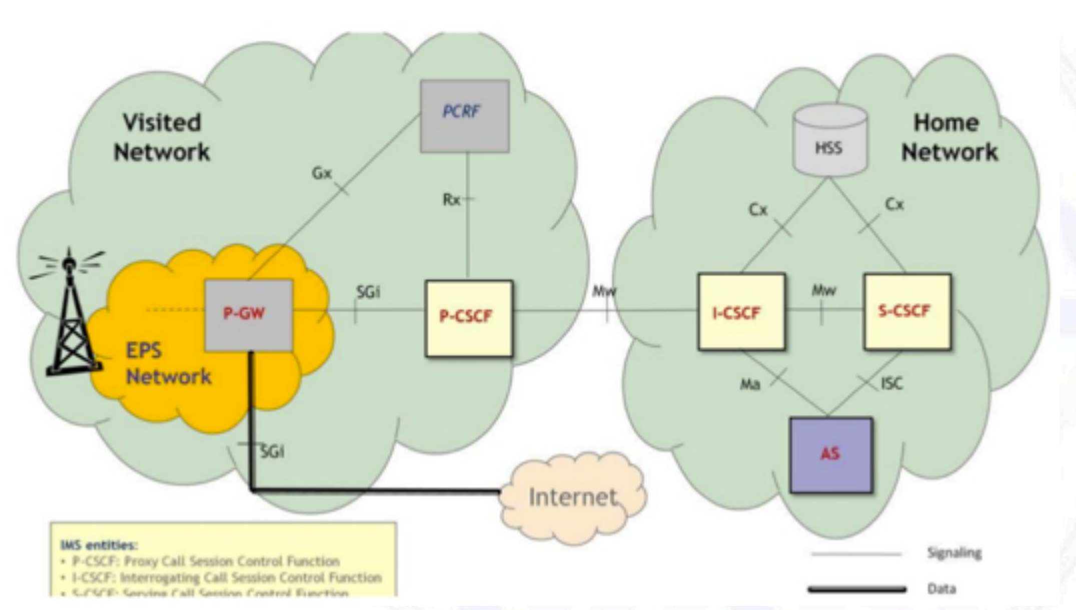


Imagen 1.35 (Arquitectura VoLTE)

El flujo completo de este tipo de comunicación VoLTE se presenta en las dos imágenes siguientes.

- UE sends SIP register req to P-CSCF
- P-CSCF finds I-CSCF, Pre configured
- I-CSCF queries HSS to find S-CSCF
- S-CSCF initiates Auth challenge

UE sends SIP Register Request to P-CSCF

Step 1: Registration Request

Step 8: Authentication Challenge

P-CSCF determines the I-CSCF (pre-configuration or via DNS)

UE has an IP address acquired via the LTE ATTACH procedure

HSS

Step 5: Authentication Vector

Step 3: Query/Response

Step 2: Registration Request

Step 7: Authentication Challenge

Step 4: Registration Request

Step 6: Authentication Challenge

S-CSCF

I-CSCF

I-CSCF assigns S-CSCF based on HSS

S-CSCF initiates AV generation and authentication

Imagen 1.36 (Flujo comunicación VoLTE)

- UE responds to Auth challenge
- SCSCF sends IMS reg'n ACK

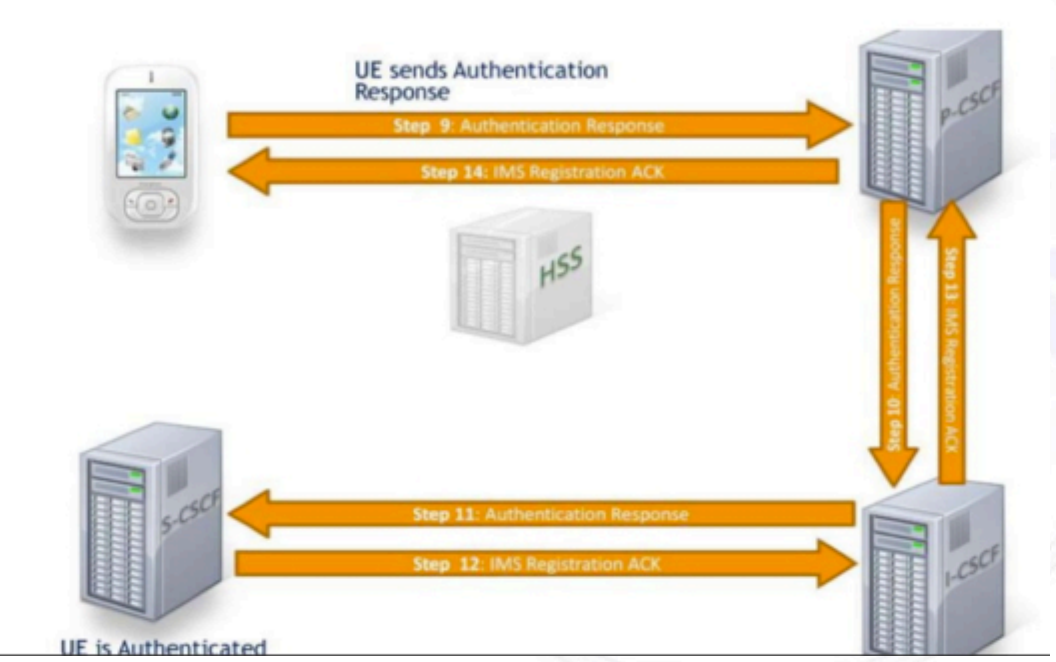


Imagen 1.37 (Flujo comunicación VoLTE)

Desde el punto de vista de SIP, este diálogo, lo podemos analizar en las siguientes dos imágenes.

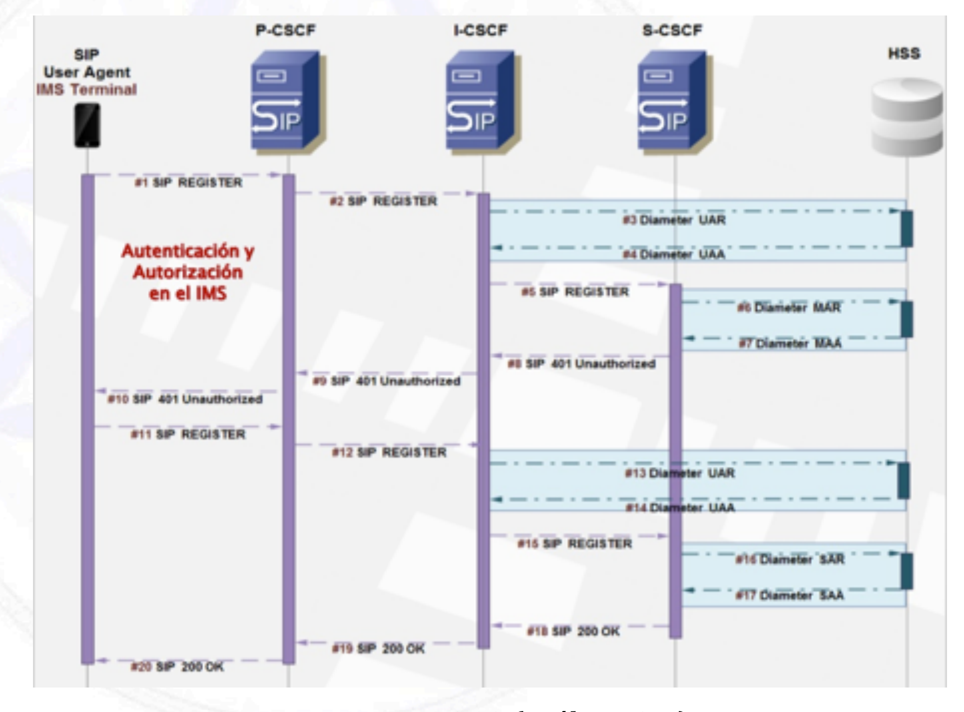


Imagen 1.38 (Diálogo SIP)



Imagen 1.39 (Diálogo SIP)

Desde el punto de vista de seguridad, lo que no podemos dejar de lado, es que en definitiva esta comunicación SIP, está viajando a través de toda nuestra red. En la imagen siguiente se presenta justamente el flujo completo de este diálogo visto de extremo a extremo.



VoLTE UE | eNB | MME | SGW | PGW | PCRF | HSS | P-CSCF | I-CSCF | S-CSCF | TAS

RRC Connection Request
RRC Connection Setup
Attach Req
Attach req - Uplink NAS Transport
RRC Connection Setup complete
[Dedicated NAS]
[PDN Connectivity Request]
[NAS PDU]
[EPS SM: PDN Connectivity Request]
Authentication/Security
Update Location Request
Update Location Answer
Create Session Request
IMS-APN; QCI:5; ARP; APN AMBR
Create Session Request
IMS-APN; QCI:5; ARP; APN AMBR
IP@; QCI:5; ARP; APN AMBR
CCR
CCA
Create Session Response
QCI:5; ARP; APN AMBR; IP default rule TFT
IP@; QCI:5; ARP; APN AMBR
Create Session Response
IP@; QCI:5; ARP; APN AMBR
E-RAB Setup
E-RAB Setup Request
QCI:5; ARP; UE AMBR
[NAS PDU]
[Activate Default Bearer Request]
[IMS-APN; IP@;]
[QCI:5; APN AMBR]
RRC Connection Reconfiguration
[NAS PDU]
[EPS SM: Activate Default Bearer Request]
RRC Connection Reconfiguration Complete
E-RAB Setup
E-RAB Setup Response
Uplink Direct Transfer
[NAS PDU]
[EPS SM: Activate Default Bearer Accept]
Attach complete - Uplink NAS Transport
[NAS PDU]
[Activate Default Bearer Accept]
Modify Bearer Request
Modify Bearer Response
Default Bearer Established for IMS Signalling
IMS Signalling over IP
SIP Register
SIP Register
UAR
UAA
SIP Register
MAR
MAA
401 Unauthorised
401 Unauthorised
401 Unauthorised
SIP Register
SIP Register
UAR
UAA
SIP Register
SAR
SAA
200 OK
200 OK
200 OK
AAR
AAA
SIP Register
UDR
UDA
200 OK
SIP Subscribe
200 OK (Subscribe)
SIP Subscribe
200 OK (Subscribe)
SIP Subscribe
200 OK (Subscribe)
SIP Subscribe
200 OK (Subscribe)
SIP Notify
200 OK (Notify)
SIP Notify
200 OK (Notify)
SIP Notify
200 OK (Notify)
SIP Notify
200 OK (Notify)

Imagen 1.40 (Flujo SIP)

SEGUNDA REFLEXIÓN DE SEGURIDAD: Como podemos apreciar en la imagen anterior, SIP nace en el UE y llega hasta el P-CSCF (*de forma directa*) pasando por eNB, MME, SGW, PGW, PCRF y HSS…… *Si no se coloca algún dispositivo intermedio*

Session Border Controller

El SBC o también conocido como SBG ("Session Border Gateway") tal cual vimos en el punto 1.7. IMS (IP Multimedia Subsystem), es el encargado de la correlación de

toda la señalización y los flujos de media (como audio y vídeo) que pasa por los extremos de la red. Este nodo proporciona acceso con seguridad, protección del ancho de banda, calidad del servicio, nivel de servicios acordados y otras funciones críticas para las transmisiones en tiempo real de audio o vídeo.

Presentamos nuevamente la figura vista en el punto mencionado:

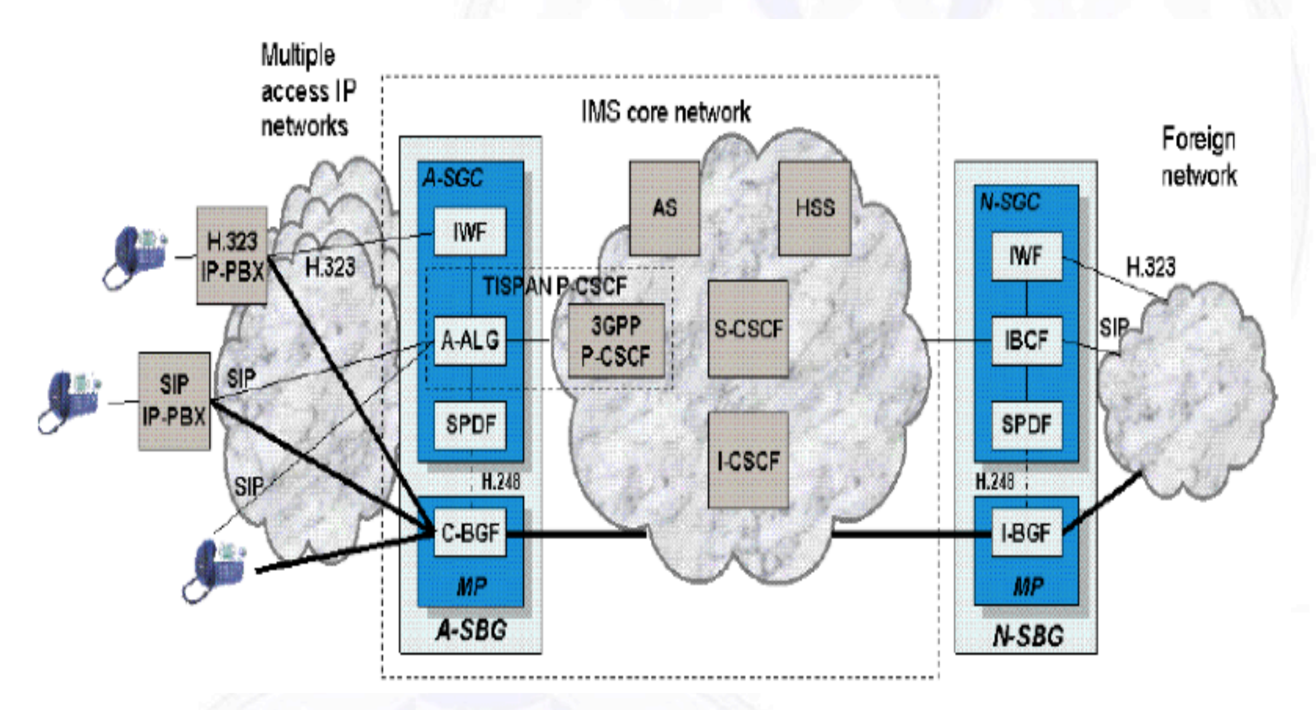


Imagen 1.41 (SBC)

Sin volver a reiterar nuevamente todos estos aspectos fundamentales desde el punto de vista de la seguridad, pasemos directamente a nuestra conclusión.

TERCERA REFLEXIÓN DE SEGURIDAD: El **SBC** es la pieza clave de la Seguridad en VoLTE.

1.8.3. Mecanismos de seguridad intrínsecos de SIP.

Volviendo a la **RFC-3261**, la misma presenta diferentes mecanismos de seguridad que "pueden" ser configurados para el empleo de SIP. A continuación los presentamos.

a. Empleo de Autenticación http.

El punto 22 de esta RFC hace referencia a la existencia de un mecanismo "básico" de autenticación y establece con total claridad que el mismo NO DEBE ser empleado (obsoleto). El mecanismo que establece para esta actividad es uno basado en "desafío" a través de un Digest que emplea MD5.

b. Empleo de S/MIME.

El cuerpo de los mensajes SIP es transportado por el protocolo MIME (Multipurpose Internet Mail Extensions). Para poder asegurar integridad y confidencialidad en estos mensajes, recomienda el empleo de S/MIME. Toda esta actividad es presentada en las RFC 1847, 2630 y 2633.

También en el punto 23.1 de la RFC-3261, desarrolla cómo implantar S/MIME a través de certificados digitales, y en el punto23.2 como aplicar "Key Exchange" para la distribución de claves públicas.

c. Empleo de túneles.

Los puntos 23.3 y 23.4 comienzan a desarrollar cómo aplicar autenticación, integridad y confidencialidad en los encabezados y el cuerpo de SIP empleando Túneles.

d. Consideraciones de seguridad.

El punto 26 describe las consideraciones de seguridad para SIP. Lo primero que establece es que "SIP no es un protocolo fácil para asegurar", justamente por la existencia de varios dispositivos intermedios, múltiples relaciones de confianza, comunicación con elementos no confiables, etc….. *"In order to meet these diverse needs, several distinct mechanisms applicable to different aspects and usages of SIP will be required"*.

Define diferentes tipos de amenazas:

- Secuestro de registro.
- Hacerse pasar por un servidor
- Manipulación de cuerpos de mensajes
- Derribar sesiones
- Denegación de servicio y amplificación

Luego de estas amenazas, en el punto 26.2 presenta los mecanismos de seguridad a nivel de transporte y de red. Los dos mecanismos para ello son:

- TLS.
- IPSec.

En el punto 26.3.2.4. Describe aspectos de protección ante DoS, empleando dominios con políticas de defensa (Bloqueos de tráfico, listas blancas y negras, filtrando ICMP, empleando TLS o IPSec, autenticación mutua entre proxies).

El punto 26.4 desarrolla todas las limitaciones de seguridad que actualmente presenta SIP: net nonce, fallos de autenticación en inter dominios, posibles ataques del hombre del medio en el proceso de autenticación, empleos de UDP o TCP, conexiones de extremo a extremo, etc.

CUARTA REFLEXIÓN DE SEGURIDAD: Se deben emplear los mecanismos de seguridad intrínseca de la RFC-3261 para el empleo de SIP.

1.8.4. Ataques a SIP.

Independientemente de los temas de seguridad que trata la RFC-3261, en la actualidad existen varios tipos de ataques comprobados y de accesible nivel de ejecución para quien desee realizarlos, en particular los ataques más difundidos son:

- Evitar facturación (el tráfico SIP no pasa por facturación).
- Manipulación de Prioridades de acceso a datos.
- DoS
- DDoS
- Sobre carga red destino
- Cancelación llamadas
- Corte de llamadas
- Escucha tráfico
- Intercepción de tráfico
- inserción de tráfico
- Ataque del hombre del medio

A continuación presentamos algunos flujos de estos ataques:

Corte de llamadas	
Figure 2. Normal session termination	Figure 3. BYE attack
Cancelación de llamadas	
Figure 4. CANCEL request	Figure 5. CANCEL attack
Re -invite	Update

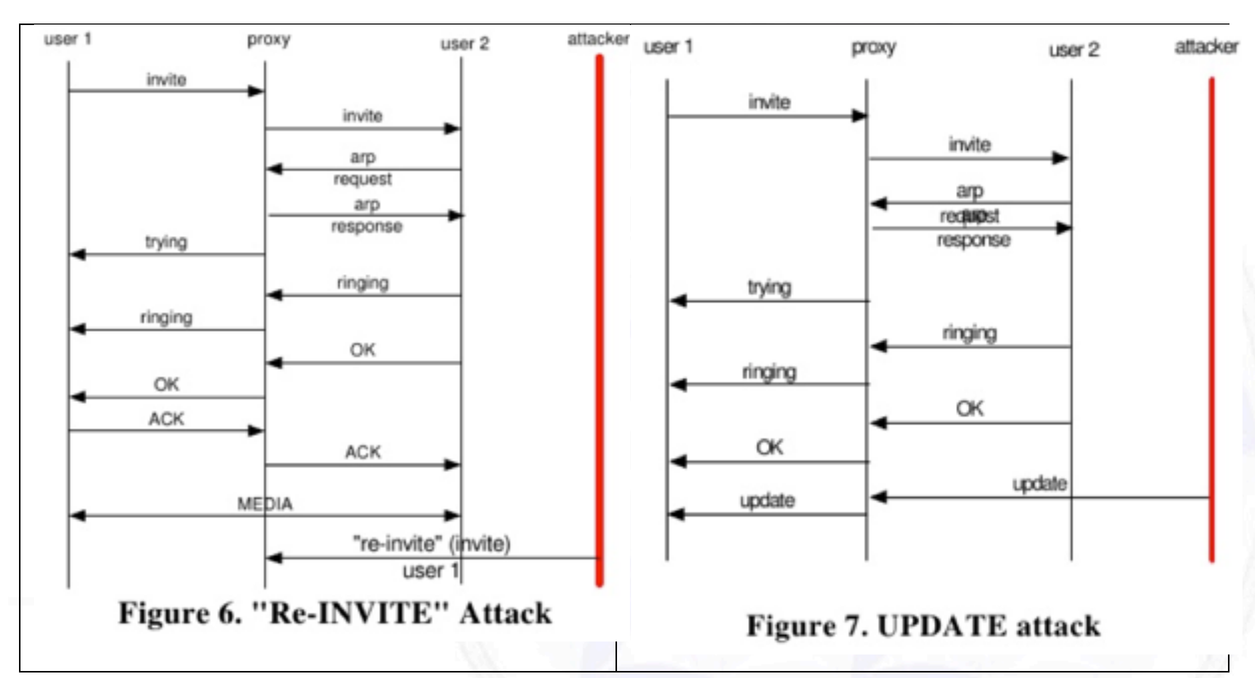
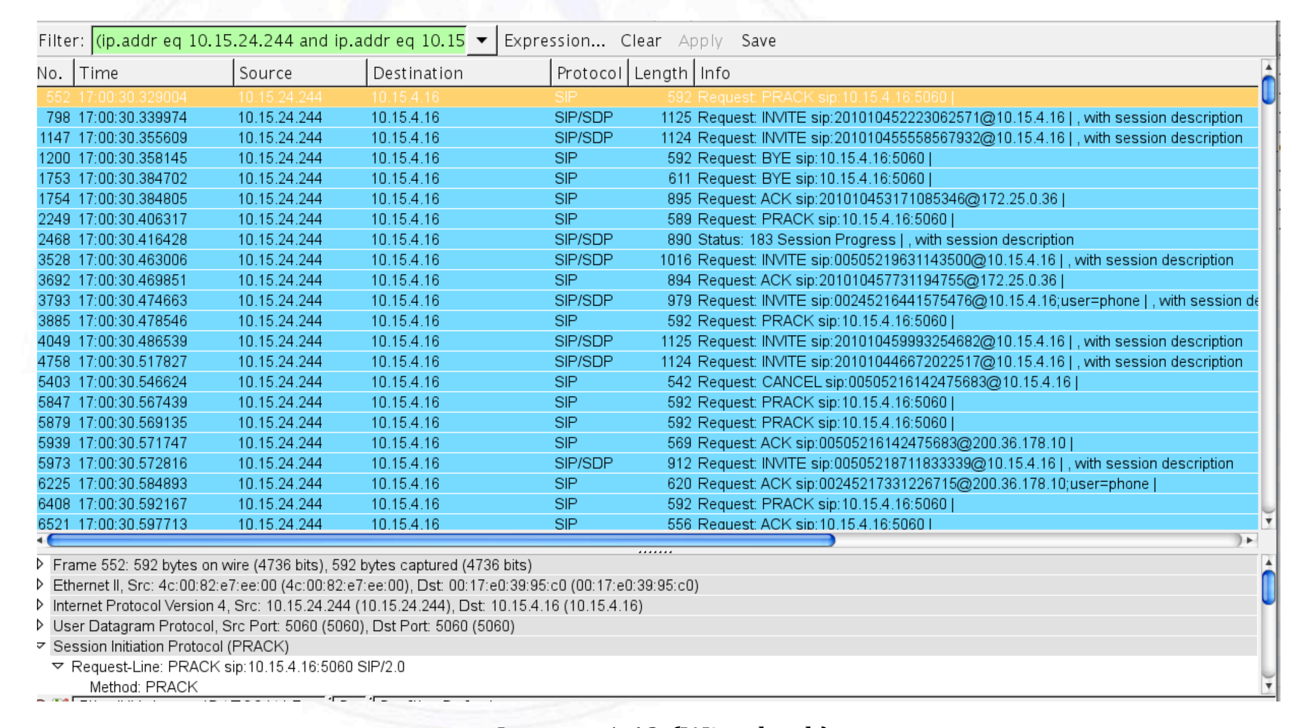


Imagen 1.42 (Ataques SIP)

Vamos a analizar el tráfico desde una central de una operadora de telefonía.

(Se presentan únicamente las imágenes, pero en la página Web de DarFe puedes descargar diferentes capturas para analizarlas con "Wireshark" de esta captura real de varias comunicaciones internacionales por medio de una infraestructura IMS y se realizarán las prácticas de inyección con némesis).



No.	Time	Source	Destination	Protocol	Length	Info
552	17:00:30.329004	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
798	17:00:30.339974	10.15.24.244	10.15.4.16	SIP/SDP	1125	Request: INVITE sip:201010452223062571@10.15.4.16 | , with session description
1147	17:00:30.355609	10.15.24.244	10.15.4.16	SIP/SDP	1124	Request: INVITE sip:201010455558567932@10.15.4.16 | , with session description
1200	17:00:30.358145	10.15.24.244	10.15.4.16	SIP	592	Request: BYE sip:10.15.4.16:5060 |
1753	17:00:30.384702	10.15.24.244	10.15.4.16	SIP	611	Request: BYE sip:10.15.4.16:5060 |
1754	17:00:30.384805	10.15.24.244	10.15.4.16	SIP	895	Request: ACK sip:201010453171085346@172.25.0.36 |
2249	17:00:30.406317	10.15.24.244	10.15.4.16	SIP	589	Request: PRACK sip:10.15.4.16:5060 |
2468	17:00:30.416428	10.15.24.244	10.15.4.16	SIP/SDP	890	Status: 183 Session Progress | , with session description
3528	17:00:30.463006	10.15.24.244	10.15.4.16	SIP/SDP	1016	Request: INVITE sip:00505219631143500@10.15.4.16 | , with session description
3692	17:00:30.469851	10.15.24.244	10.15.4.16	SIP	894	Request: ACK sip:201010457731194755@172.25.0.36 |
3793	17:00:30.474663	10.15.24.244	10.15.4.16	SIP/SDP	979	Request: INVITE sip:00245216441575476@10.15.4.16;user=phone | , with session de
3885	17:00:30.478546	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
4049	17:00:30.486539	10.15.24.244	10.15.4.16	SIP/SDP	1125	Request: INVITE sip:201010459993254682@10.15.4.16 | , with session description
4758	17:00:30.517827	10.15.24.244	10.15.4.16	SIP/SDP	1124	Request: INVITE sip:201010446672022517@10.15.4.16 | , with session description
5403	17:00:30.546624	10.15.24.244	10.15.4.16	SIP	542	Request: CANCEL sip:00505216142475683@10.15.4.16 |
5847	17:00:30.567439	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
5879	17:00:30.569135	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
5939	17:00:30.571747	10.15.24.244	10.15.4.16	SIP	569	Request: ACK sip:00505216142475683@200.36.178.10 |
5973	17:00:30.572816	10.15.24.244	10.15.4.16	SIP/SDP	912	Request: INVITE sip:00505218711833339@10.15.4.16 | , with session description
6225	17:00:30.584893	10.15.24.244	10.15.4.16	SIP	620	Request: ACK sip:00245217331226715@200.36.178.10;user=phone |
6408	17:00:30.592167	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
6521	17:00:30.597713	10.15.24.244	10.15.4.16	SIP	556	Request: ACK sip:10.15.4.16:5060 |

Frame 552: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits)
Ethernet II, Src: 4c:00:82:e7:ee:00 (4c:00:82:e7:ee:00), Dst: 00:17:e0:39:95:c0 (00:17:e0:39:95:c0)
Internet Protocol Version 4, Src: 10.15.24.244 (10.15.24.244), Dst: 10.15.4.16 (10.15.4.16)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol (PRACK)
Request-Line: PRACK sip:10.15.4.16:5060 SIP/2.0
Method: PRACK

Imagen 1.43 (Wireshark)

De este tráfico real, seleccionamos (exportamos) sólo una trama "INVITE".

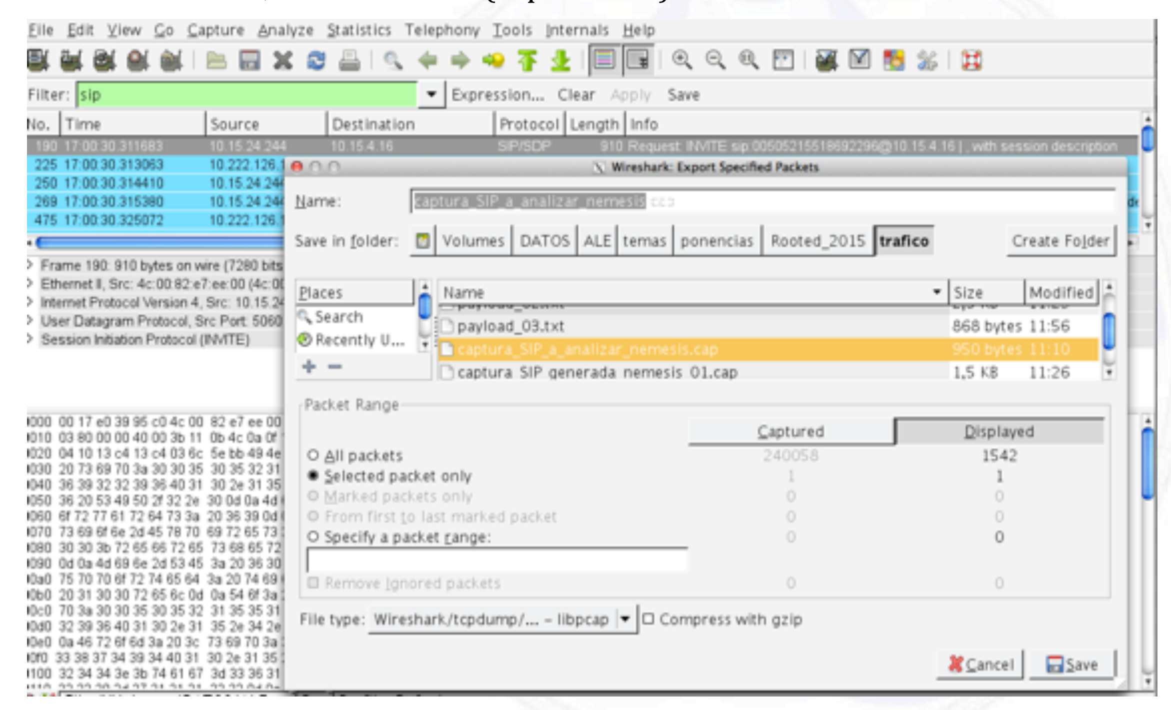


Imagen 1.44 (Wireshark)

Para un mejor análisis y trabajo con las misma, desde Wireshark también la "Imprimimos" en formato texto, y nos queda como se presenta a continuación (Algún dato de numeración telefónica ha sido modificada par ocultar datos reales):

No. Time Source Destination Protocol Length Info
1 :00:30.311683 10.15.24.244 10.15.4.16 SIP/SDP 910 Request: INVITE sip:00605215518692396@10.15.4.16 | , with session description

Frame 1: 910 bytes on wire (7280 bits), 910 bytes captured (7280 bits)
WTAP_ENCAP: 1
Arrival Time: Jul 25, 2014 17:00:30.311683000 CEST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1406300430.311683000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 910 bytes (7280 bits)
Capture Length: 910 bytes (7280 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:udp:sip:sdp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: 4c:00:82:e7:ee:00 (4c:00:82:e7:ee:00), Dst: 00:17:e0:39:95:c0 (00:17:e0:39:95:c0)

```
  Destination: 00:17:e0:39:95:c0 (00:17:e0:39:95:c0)
    Address: 00:17:e0:39:95:c0 (00:17:e0:39:95:c0)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: 4c:00:82:e7:ee:00 (4c:00:82:e7:ee:00)
    Address: 4c:00:82:e7:ee:00 (4c:00:82:e7:ee:00)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.15.24.244 (10.15.24.244), Dst: 10.15.4.16 (10.15.4.16)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-
Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 896
  Identification: 0x0000 (0)
  Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 59
  Protocol: UDP (17)
  Header checksum: 0x0b4c [correct]
    [Good: True]
    [Bad: False]
  Source: 10.15.24.244 (10.15.24.244)
  Destination: 10.15.4.16 (10.15.4.16)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
  Source port: 5060 (5060)
  Destination port: 5060 (5060)
  Length: 876
  Checksum: 0x5ebb [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip: 00605215518692366@10.15.4.16 SIP/2.0
    Method: INVITE
    Request-URI: sip: 00605215518692366@10.15.4.16
      Request-URI User Part: 00605215518692366
      Request-URI Host Part: 10.15.4.16
    [Resent Packet: False]
  Message Header
    Max-Forwards: 69
    Session-Expires: 3600;refresher=uac
    Min-SE: 600
    Supported: timer, 100rel
    To: <sip: 00605215518692366@10.15.4.16>
      SIP to address: sip: 00605215518692366@10.15.4.16
        SIP to address User Part: 00605215518692366
        SIP to address Host Part: 10.15.4.16
    From: <sip:3466387494@10.15.24.244>;tag=3615289230-711133
```

SIP from address: sip:3766387494@10.15.24.244
SIP from address User Part: 3766387494
SIP from address Host Part: 10.15.24.244
SIP from tag: 3615289230-711133
Call-ID: 753261-3615289230-711129@MY-BMS-01D.datos.tss
CSeq: 1 INVITE
Sequence Number: 1
Method: INVITE
Allow: CANCEL, ACK, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP 10.15.24.244:5060;branch=z9hG4bK9b39c13355d40025c8ae6fb918f289b8
Transport: UDP
Sent-by Address: 10.15.24.244
Sent-by port: 5060
Branch: z9hG4bK9b39c13355d40025c8ae6fb918f289b8
Contact: <sip:3766387494@10.15.24.244:5060>
Contact URI: sip:3766387494@10.15.24.244:5060
Contact URI User Part: 3766387494
Contact URI Host Part: 10.15.24.244
Contact URI Host Port: 5060
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 227
Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): M-BM-01D 188 1 IN IP4 10.15.24.244
Owner Username: M-BM-01D
Session ID: 188
Session Version: 1
Owner Network Type: IN
Owner Address Type: IP4
Owner Address: 10.15.24.244
Session Name (s): sip call
Connection Information (c): IN IP4 10.15.24.245
Connection Network Type: IN
Connection Address Type: IP4
Connection Address: 10.15.24.245
Time Description, active time (t): 0 0
Session Start Time: 0
Session Stop Time: 0
Media Description, name and address (m): audio 23766 RTP/AVP 18 101
Media Type: audio
Media Port: 23766
Media Protocol: RTP/AVP
Media Format: ITU-T G.729
Media Format: DynamicRTP-Type-101
Media Attribute (a): rtpmap:18 G729/8000
Media Attribute FielAQ1me: rtpmap
Media Format: 18
MIME Type: G729
Sample Rate: 8000
Media Attribute (a): fmtp:18 annexb=no
Media Attribute FielAQ1me: fmtp
Media Format: 18 [G729]






```
        Media format specific parameters: annexb=no
      Media Attribute (a): rtpmap:101 telephone-event/8000
        Media Attribute FielAQ1me: rtpmap
        Media Format: 101
        MIME Type: telephone-event
        Sample Rate: 8000
      Media Attribute (a): fmtp:101 0-15
        Media Attribute FielAQ1me: fmtp
        Media Format: 101 [telephone-event]
        Media format specific parameters: 0-15
      Media Attribute (a): ptime:20
        Media Attribute FielAQ1me: ptime
        Media Attribute Value: 20

0000  00 17 e0 39 95 c0 4c 00 82 e7 ee 00 08 00 45 00   ...9..L.......E.
0010  03 80 00 00 40 00 3b 11 0b 4c 0a 0f 18 f4 0a 0f   ....@.;..L......
0020  04 10 13 c4 13 c4 03 6c 5e bb 49 4e 56 49 54 45   .......l^.INVITE
0030  20 73 69 70 3a 30 30 35 30 35 32 31 35 35 31 38    sip:00605215518
0040  36 39 32 32 39 36 40 31 30 2e 31 35 2e 34 2e 31   692366@10.15.4.1
0050  36 20 53 49 50 2f 32 2e 30 0d 0a 4d 61 78 2d 46   6 SIP/2.0..Max-F
0060  6f 72 77 61 72 64 73 3a 20 36 39 0d 0a 53 65 73   orwards: 69..Ses
0070  73 69 6f 6e 2d 45 78 70 69 72 65 73 3a 20 33 36   sion-Expires: 36
0080  30 30 3b 72 65 66 72 65 73 68 65 72 3d 75 61 63   00;refresher=uac
0090  0d 0a 4d 69 6e 2d 53 45 3a 20 36 30 30 0d 0a 53   ..Min-SE: 600..S
00a0  75 70 70 6f 72 74 65 64 3a 20 74 69 6d 65 72 2c   upported: timer,
00b0  20 31 30 30 72 65 6c 0d 0a 54 6f 3a 20 3c 73 69    100rel..To: <si
00c0  70 3a 30 30 35 30 35 32 31 35 35 31 38 36 39 32   p:00605215518692
00d0  32 39 36 40 31 30 2e 31 35 2e 34 2e 31 36 3e 0d   366@10.15.4.16>.
00e0  0a 46 72 6f 6d 3a 20 3c 73 69 70 3a 33 34 37 37   .From: <sip:3766
00f0  33 38 37 34 39 34 40 31 30 2e 31 35 2e 32 34 2e   387494@10.15.24.
0100  32 34 34 3e 3b 74 61 67 3d 33 36 31 35 32 38 39   244>;tag=3615289
0110  32 33 30 2d 37 31 31 31 33 33 0d 0a 43 61 6c 6c   230-711133..Call
0120  2d 49 44 3a 20 37 35 33 32 36 31 2d 33 36 31 35   -ID: 753261-3615
0130  32 38 39 32 33 30 2d 37 31 31 31 32 39 40 4d 54   289230-711129@M
0140  59 2d 42 4d 53 57 2d 30 31 44 2e 64 61 74 6f 73   Y-BMS-01D.datos
0150  2e 74 65 6d 6d 0d 0a 43 53 65 71 3a 20 31 20 49   .tss...CSeq: 1 I
0160  4e 56 49 54 45 0d 0a 41 6c 6c 6f 77 3a 20 43 41   NVITE..Allow: CA
0170  4e 43 45 4c 2c 20 41 43 4b 2c 20 49 4e 56 49 54   NCEL, ACK, INVIT
0180  45 2c 20 42 59 45 2c 20 4f 50 54 49 4f 4e 53 2c   E, BYE, OPTIONS,
0190  20 52 45 47 49 53 54 45 52 2c 20 4e 4f 54 49 46    REGISTER, NOTIF
01a0  59 2c 20 49 4e 46 4f 2c 20 52 45 46 45 52 2c 20   Y, INFO, REFER,
01b0  53 55 42 53 43 52 49 42 45 2c 20 50 52 41 43 4b   SUBSCRIBE, PRACK
01c0  2c 20 55 50 44 41 54 45 2c 20 4d 45 53 53 41 47   , UPDATE, MESSAG
01d0  45 2c 20 50 55 42 4c 49 53 48 0d 0a 56 69 61 3a   E, PUBLISH..Via:
01e0  20 53 49 50 2f 32 2e 30 2f 55 44 50 20 31 30 2e    SIP/2.0/UDP 10.
01f0  31 35 2e 32 34 2e 32 34 34 3a 35 30 36 30 3b 62   15.24.244:5060;b
0200  72 61 6e 63 68 3d 7a 39 68 47 34 62 4b 39 62 33   ranch=z9hG4bK9b3
0210  39 63 31 33 33 35 35 64 34 30 30 32 35 63 38 61   9c13355d40025c8a
0220  65 36 66 62 39 31 38 66 32 38 39 62 38 0d 0a 43   e6fb918f289b8..C
0230  6f 6e 74 61 63 74 3a 20 3c 73 69 70 3a 33 34 37   ontact: <sip:377
0240  37 33 38 37 34 39 34 40 31 30 2e 31 35 2e 32 34   7387494@10.15.24
0250  2e 32 34 34 3a 35 30 36 30 3e 0d 0a 43 6f 6e 74   .244:5060>..Cont
0260  65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63   ent-Type: applic
0270  61 74 69 6f 6e 2f 73 64 70 0d 0a 41 63 63 65 70   ation/sdp..Accep
0280  74 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73   t: application/s
0290  64 70 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67   dp..Content-Leng
```

```
02a0  74 68 3a 20 32 32 37 0d 0a 0d 0a 76 3d 30 0d 0a   th: 227....v=0..
02b0  6f 3d 4d 54 59 2d 42 4d 53 57 2d 30 31 44 20 31   o=M-BM-01D 1
02c0  38 38 20 31 20 49 4e 20 49 50 34 20 31 30 2e 31   88 1 IN IP4 10.1
02d0  35 2e 32 34 2e 32 34 34 0d 0a 73 3d 73 69 70 20   5.24.244..s=sip
02e0  63 61 6c 6c 0d 0a 63 3d 49 4e 20 49 50 34 20 31   call..c=IN IP4 1
02f0  30 2e 31 35 2e 32 34 2e 32 34 35 0d 0a 74 3d 30   0.15.24.245..t=0
0300  20 30 0d 0a 6d 3d 61 75 64 69 6f 20 32 33 37 36    0..m=audio 2376
0310  36 20 52 54 50 2f 41 56 50 20 31 38 20 31 30 31   6 RTP/AVP 18 101
0320  0d 0a 61 3d 72 74 70 6d 61 70 3a 31 38 20 47 37   ..a=rtpmap:18 G7
0330  32 39 2f 38 30 30 30 0d 0a 61 3d 66 6d 74 70 3a   29/8000..a=fmtp:
0340  31 38 20 61 6e 6e 65 78 62 3d 6e 6f 0d 0a 61 3d   18 annexb=no..a=
0350  72 74 70 6d 61 70 3a 31 30 31 20 74 65 6c 65 70   rtpmap:101 telep
0360  68 6f 6e 65 2d 65 76 65 6e 74 2f 38 30 30 30 0d   hone-event/8000.
0370  0a 61 3d 66 6d 74 70 3a 31 30 31 20 30 2d 31 35   .a=fmtp:101 0-15
0380  0d 0a 61 3d 70 74 69 6d 65 3a 32 30 0d 0a         ..a=ptime:20..
```

Lo que nos interesa para poder trabajar son las direcciones IP, sus Flags, puertos UDP y payload:

```
Src: 10.15.24.244 (10.15.24.244)
Dst: 10.15.4.16 (10.15.4.16)
   Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
   Source port: 5060 (5060)
   Destination port: 5060 (5060)
```

Del "Payload", lo que necesitamos para poder generar tráfico con "nemesis" es la parte de la derecha de la presentación formato ".cap" como se presenta en la imagen que sigue:

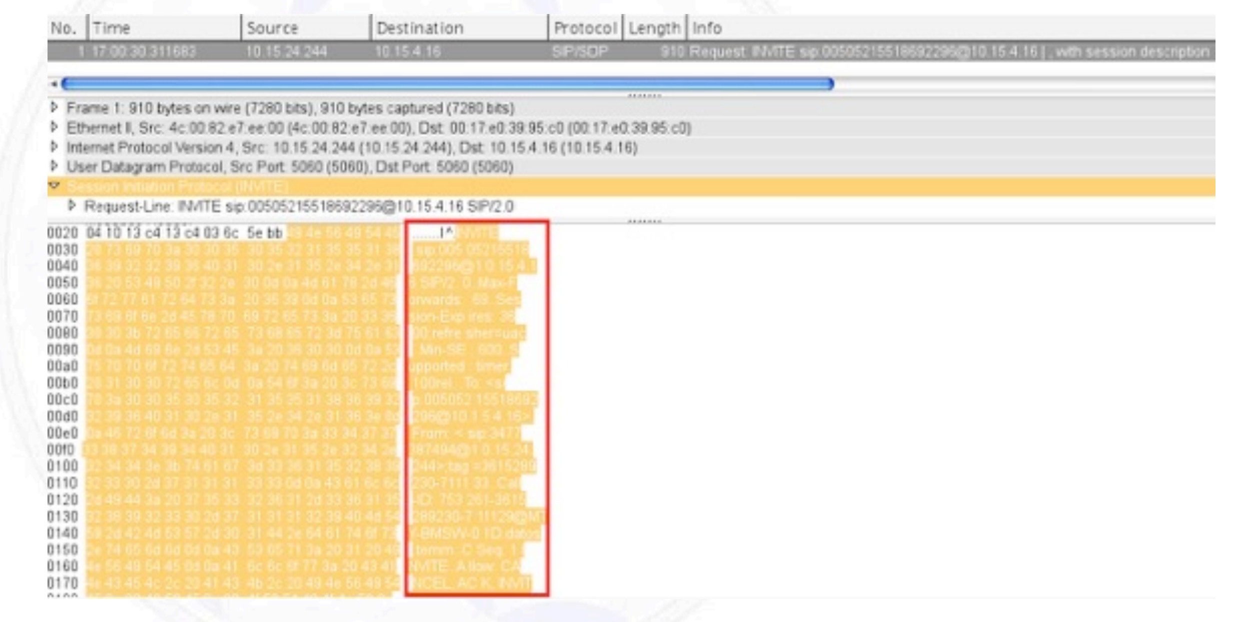


Imagen 1.45 (Wireshark campo payload)

Lo cual al tener la trama completa en formato de texto, deberemos filtrar sólo ese contenido, el cual nos queda como se presenta a continuación:

INVITE sip:00505215518692266@10.15.4.16 SIP/2.0..Max-Forwards: 69..Session-Expires: 3600;refresher=uac..Min-SE: 600..Supported: timer, 100rel..To: <sip:00505215518692266@10.15.4.16>..From: <sip:3777387494@10.15.24.244>;tag=3615289230-711133..Call-ID: 753261-3615289230-711129@M-BM-01D.datos.tss..CSeq: 1 INVITE..Allow: CANCEL, ACK, INVITE, BYE, OPTIONS,REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH..Via: SIP/2.0/UDP 10.15.24.244:5060;branch=z9hG4bK9b39c13355d40025c8ae6fb918f289b8..Contact: <sip:3777387494@10.15.24.244:5060>..Content-Type: application/sdp..Accept: application/sdp..Content-Length: 227....v=0..o=MY-BMS-01D 188 1 IN IP4 10.15.24.244..s=sip call..c=IN IP4 10.15.24.245..t=0 0..m=audio 23766 RTP/AVP 18 101..a=rtpmap:18 G729/8000..a=fmtp: 18 annexb=no..a=rtpmap:101 telephone-event/8000..a=fmtp:101 0-15..a=ptime:20..

Este archivo de texto, lo podemos guardar con cualquier nombre, en nuestro caso lo llamaremos "payload_03.txt" y nos servirá para poder comenzar a trabajar con el software "**nemesis**" en la generación de tráfico.

Para poder generar una trama exactamente igual (desde el nivel 3, considerando su control de errores) el comando que debemos ejecutar es:

sh-3.2# nemesis udp -v -d en0 -D 10.15.4.16 -y 5060 -FD -S 10.15.24.144 -x 5060 -P payload_03.txt

A continuación se presenta la captura con Wireshark de esta trama, en la cual podemos ver que es exactamente igual a la capturada en el tráfico real:

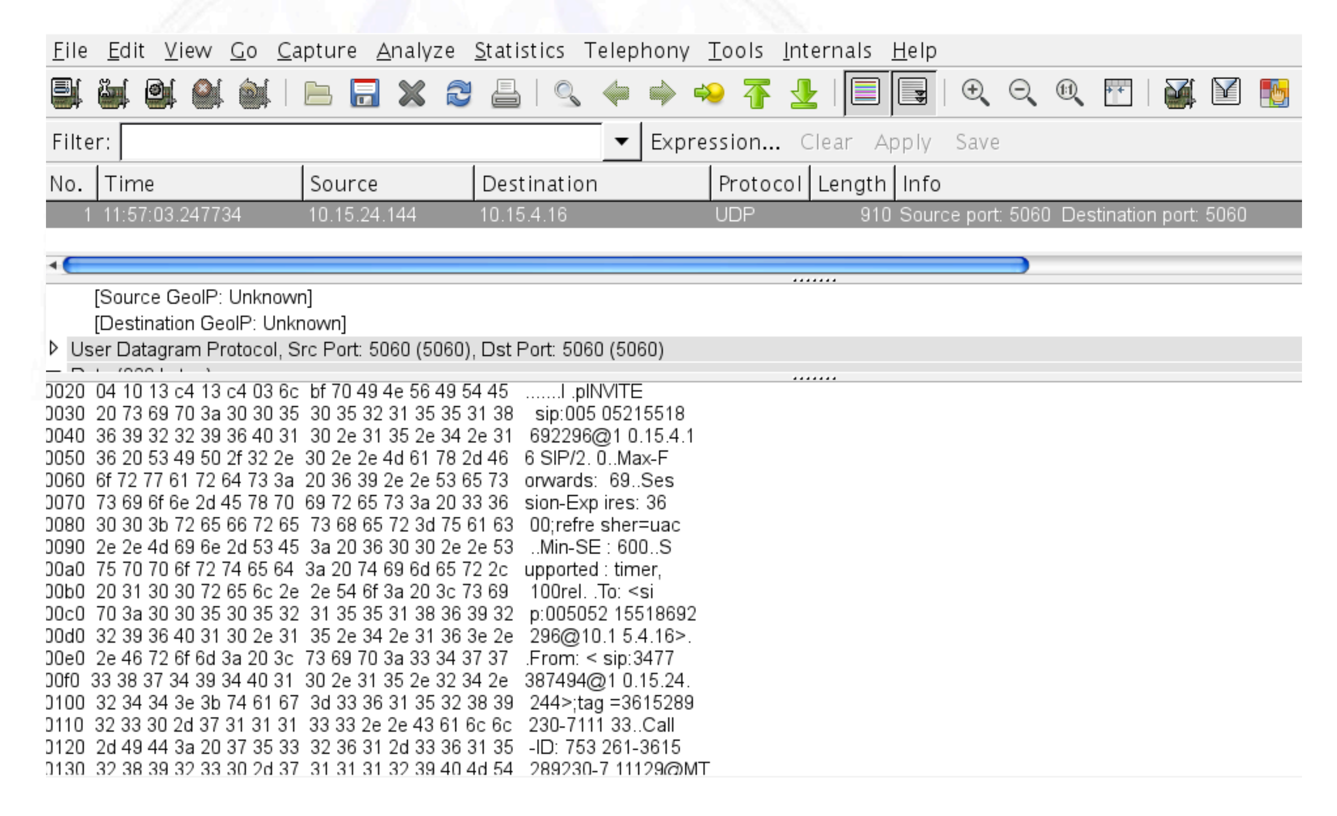
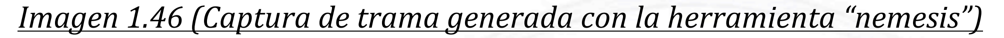


Imagen 1.46 (Captura de trama generada con la herramienta "nemesis")



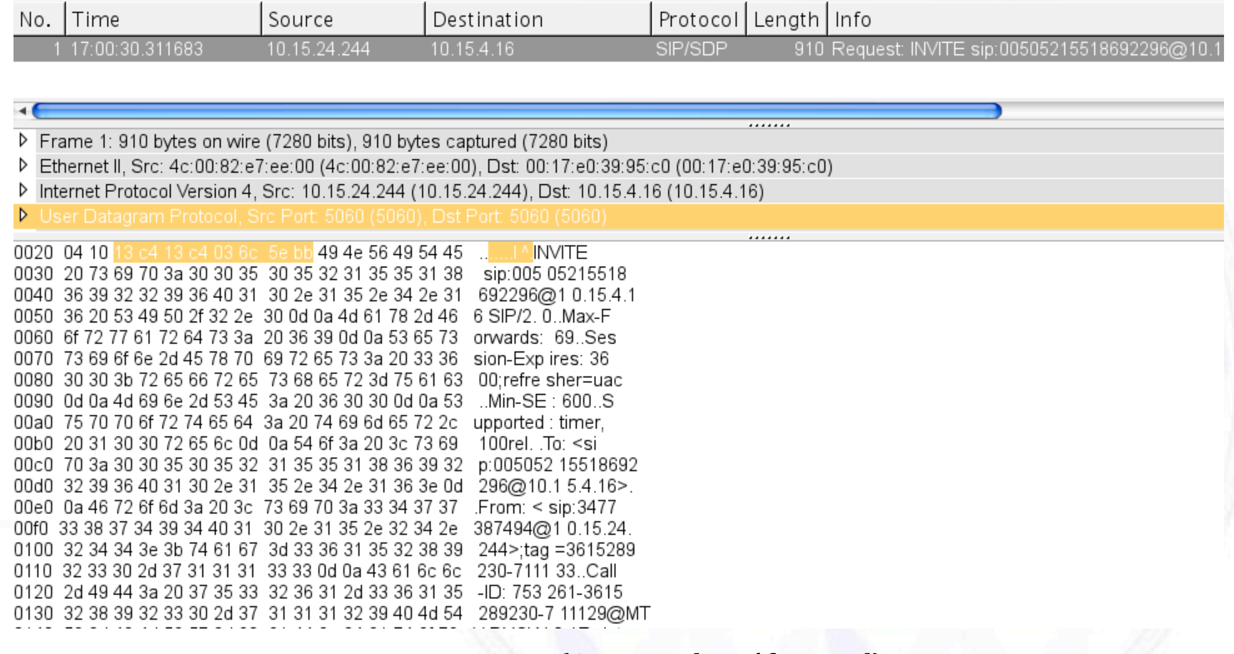


Imagen 1.47 (Captura de tráfico real)

A partir de ahora, todo el trabajo que se puede realizar es por medio de este "Payload" con el cual cambiando cualquiera de los parámetros del encabezado SIP, podemos generar el tipo de trama que deseemos.

Existen otro tipo de herramientas para esta actividad que figuran a continuación, pero se presentó en primer término "nemesis" pues por tratarse de línea de comandos, ofrece mucha mayor potencia en la generación de tráfico.

Existen muchas más, pero a continuación sólo se presentan dos de ellas:

Una de ellas, específica para trafico SIP es "**SipScan**":



Imagen 1.48 (SipScan)

La otra que puede emplearse también es “Packet Builder”:

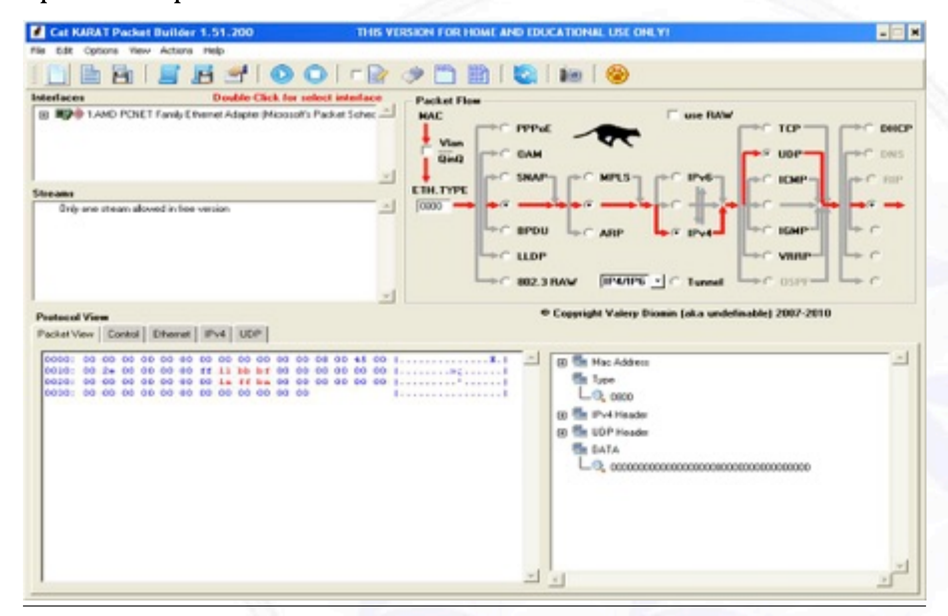


Imagen 1.49 (Packet Builder)

Para comenzar a analizar y realizar pruebas de tráfico SIP, tal vez el mejor punto de partida sea crear nuestra propia infraestructura de VoIP o conectarnos a cualquier red de VoIP con nuestra portátil. El método más sencillo para capturar y analizar este tráfico es obligando a pasar por nuestro ordenador las tramas que deseemos analizar, para ello en este caso proponemos el empleo de “Cain”, y la mejor estrategia para forzar el pasaje de este tráfico por nosotros es a través del conocido ataque “del hombre del medio” para el cual necesitamos envenenar la caché ARP del proxy de nuestra red, para que redirija todo el tráfico del teléfono deseado a hacia nuestra tarjeta MAC, lo mismo se realiza siguiendo los pasos que se presentan a continuación:

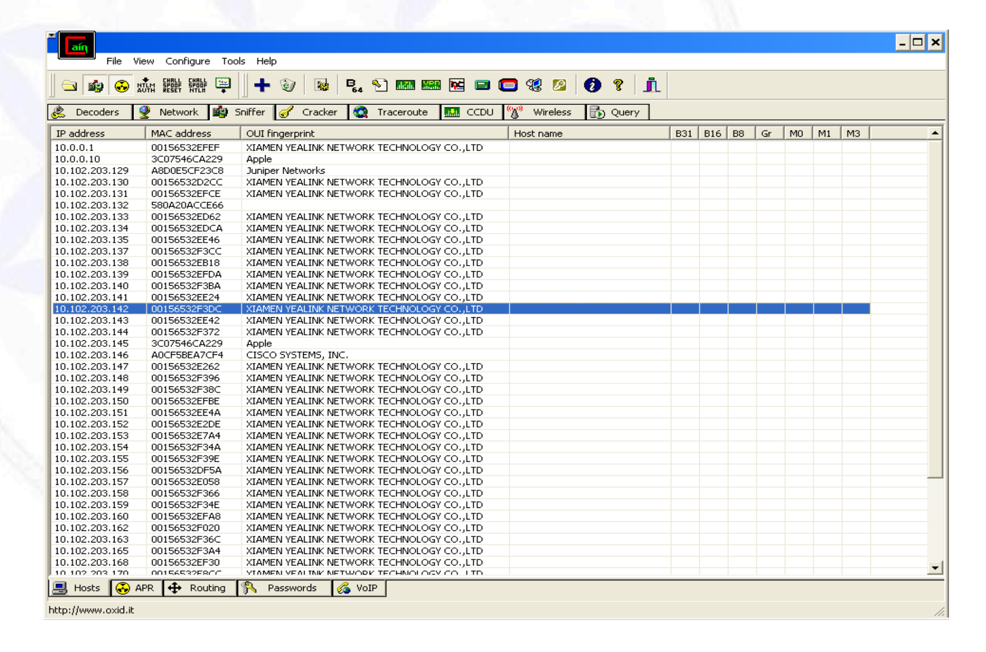


Imagen 1.50 (Cain)

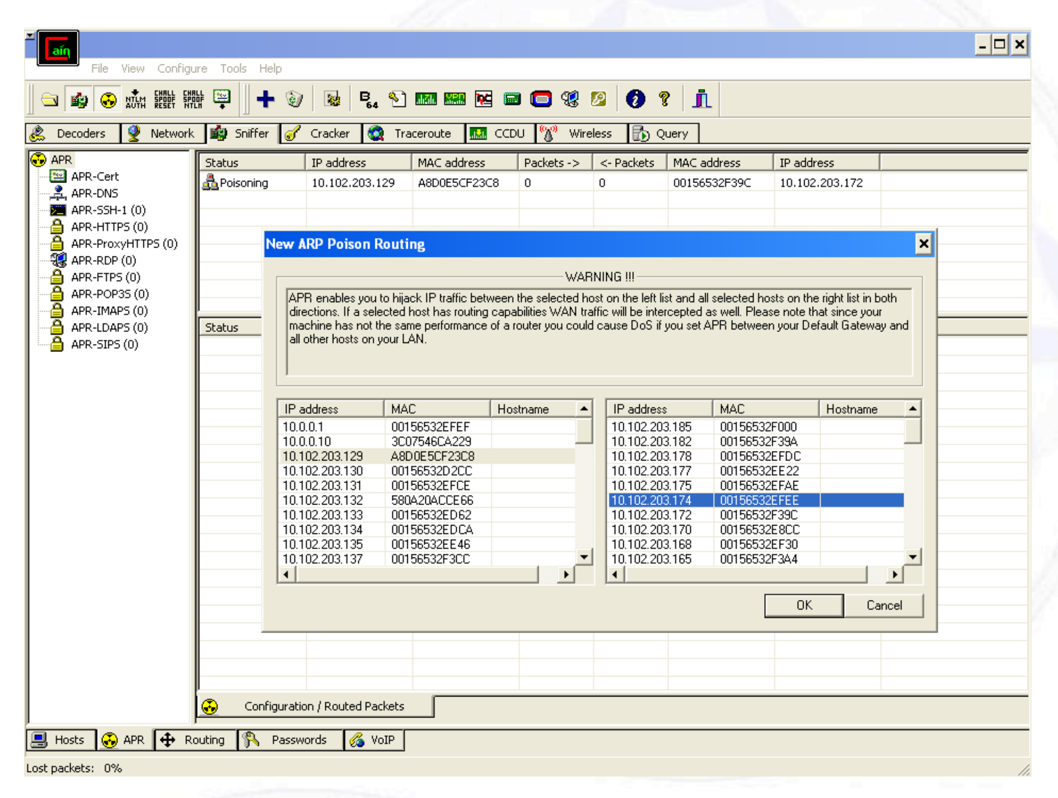


Imagen 1.51 (Cain)

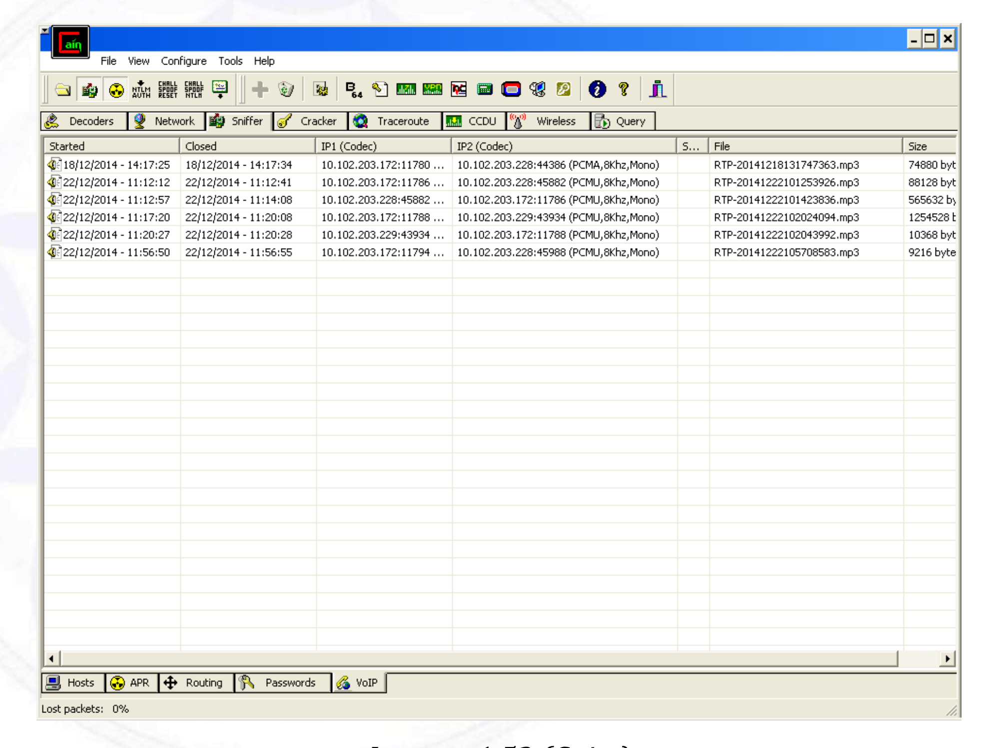


Imagen 1.52 (Cain)

Si esta actividad la vamos combinando con el empleo de **nmap** y **Wireshark**, nuestra evaluación puede quedar totalmente completa, a continuación, se presentan algunas imágenes de esta tarea.

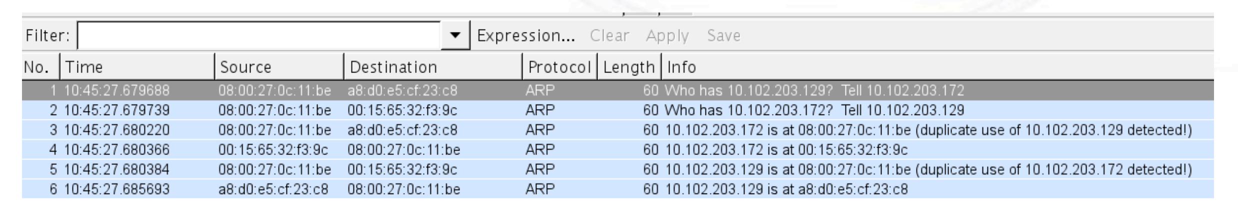
Con "nmap" podemos obtener la relación de todos los teléfonos IP y su direcciones MAC para poder realizar el envenenamiento al que deseemos, luego consultando nuestra caché ARP obtenemos la información deseada:

```
sh-3.2# arp -an
? (10.102.203.128) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (10.102.203.129) at a8:d0:e5:cf:23:c8 on en0 ifscope [ethernet]
? (10.102.203.130) at 0:15:65:32:d2:cc on en0 ifscope [ethernet]
? (10.102.203.131) at 0:15:65:32:ef:ce on en0 ifscope [ethernet]
? (10.102.203.132) at 58:a:20:ac:ce:66 on en0 ifscope [ethernet]
? (10.102.203.133) at 0:15:65:32:ed:62 on en0 ifscope [ethernet]
? (10.102.203.134) at 0:15:65:32:ed:ca on en0 ifscope [ethernet]
? (10.102.203.135) at 0:15:65:32:ee:46 on en0 ifscope [ethernet]
? (10.102.203.136) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.137) at 0:15:65:32:f3:cc on en0 ifscope [ethernet]
? (10.102.203.138) at 0:15:65:32:eb:18 on en0 ifscope [ethernet]
? (10.102.203.139) at 0:15:65:32:ef:da on en0 ifscope [ethernet]
? (10.102.203.140) at 0:15:65:32:f3:ba on en0 ifscope [ethernet]
? (10.102.203.141) at 0:15:65:32:ee:24 on en0 ifscope [ethernet]
? (10.102.203.142) at 0:15:65:32:f3:dc on en0 ifscope [ethernet]
? (10.102.203.143) at 0:15:65:32:ee:42 on en0 ifscope [ethernet]
? (10.102.203.144) at 0:15:65:32:f3:72 on en0 ifscope [ethernet]
? (10.102.203.146) at a0:cf:5b:ea:7c:f4 on en0 ifscope [ethernet]
? (10.102.203.147) at 0:15:65:32:e2:62 on en0 ifscope [ethernet]
? (10.102.203.148) at 0:15:65:32:f3:96 on en0 ifscope [ethernet]
? (10.102.203.149) at 0:15:65:32:f3:8c on en0 ifscope [ethernet]
? (10.102.203.150) at 0:15:65:32:ef:be on en0 ifscope [ethernet]
? (10.102.203.151) at 0:15:65:32:ee:4a on en0 ifscope [ethernet]
? (10.102.203.152) at 0:15:65:32:e2:de on en0 ifscope [ethernet]
? (10.102.203.153) at 0:15:65:32:e7:a4 on en0 ifscope [ethernet]
? (10.102.203.154) at 0:15:65:32:f3:4a on en0 ifscope [ethernet]
? (10.102.203.155) at 0:15:65:32:f3:9e on en0 ifscope [ethernet]
? (10.102.203.156) at 0:15:65:32:df:5a on en0 ifscope [ethernet]
? (10.102.203.157) at 0:15:65:32:e0:58 on en0 ifscope [ethernet]
? (10.102.203.158) at 0:15:65:32:f3:66 on en0 ifscope [ethernet]
? (10.102.203.159) at 0:15:65:32:f3:4e on en0 ifscope [ethernet]
? (10.102.203.160) at 0:15:65:32:ef:a8 on en0 ifscope [ethernet]
? (10.102.203.161) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.162) at 0:15:65:32:f0:20 on en0 ifscope [ethernet]
? (10.102.203.163) at 0:15:65:32:f3:6c on en0 ifscope [ethernet]
? (10.102.203.164) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.165) at 0:15:65:32:f3:a4 on en0 ifscope [ethernet]
? (10.102.203.166) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.167) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.168) at 0:15:65:32:ef:30 on en0 ifscope [ethernet]
? (10.102.203.169) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.170) at 0:15:65:32:e8:cc on en0 ifscope [ethernet]
? (10.102.203.171) at 0:15:65:32:f3:48 on en0 ifscope [ethernet]
? (10.102.203.172) at 0:15:65:32:f3:9c on en0 ifscope [ethernet]
```

```
? (10.102.203.173) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.174) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.175) at 0:15:65:32:ef:ae on en0 ifscope [ethernet]
? (10.102.203.176) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.177) at 0:15:65:32:ee:22 on en0 ifscope [ethernet]
? (10.102.203.178) at 0:15:65:32:ef:dc on en0 ifscope [ethernet]
? (10.102.203.179) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.180) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.181) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.182) at 0:15:65:32:f3:9a on en0 ifscope [ethernet]
? (10.102.203.183) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.184) at 0:15:65:32:ed:f6 on en0 ifscope [ethernet]
? (10.102.203.185) at 0:15:65:32:f0:0 on en0 ifscope [ethernet]
? (10.102.203.186) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.187) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.188) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.189) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.190) at (incomplete) on en0 ifscope [ethernet]
? (10.102.203.191) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
```

Con **Wireshark** podemos analizar todo el tráfico deseado.

La primera imagen nos presenta la secuencia de envenenamiento ARP:

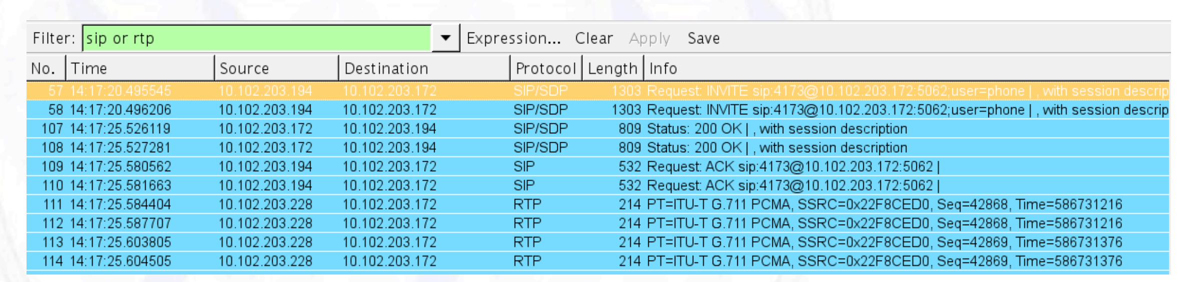


Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	10:45:27.679688	08:00:27:0c:11:be	a8:d0:e5:cf:23:c8	ARP	60	Who has 10.102.203.129? Tell 10.102.203.172
2	10:45:27.679739	08:00:27:0c:11:be	00:15:65:32:f3:9c	ARP	60	Who has 10.102.203.172? Tell 10.102.203.129
3	10:45:27.680220	08:00:27:0c:11:be	a8:d0:e5:cf:23:c8	ARP	60	10.102.203.172 is at 08:00:27:0c:11:be (duplicate use of 10.102.203.129 detected!)
4	10:45:27.680366	00:15:65:32:f3:9c	08:00:27:0c:11:be	ARP	60	10.102.203.172 is at 00:15:65:32:f3:9c
5	10:45:27.680384	08:00:27:0c:11:be	00:15:65:32:f3:9c	ARP	60	10.102.203.129 is at 08:00:27:0c:11:be (duplicate use of 10.102.203.172 detected!)
6	10:45:27.685693	a8:d0:e5:cf:23:c8	08:00:27:0c:11:be	ARP	60	10.102.203.129 is at a8:d0:e5:cf:23:c8

Imagen 1.53 (Wireshark)

A continuación hemos filtrado una captura para visualizar sólo el tráfico SIP y RTP:



Filter: sip or rtp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
57	14:17:20.495545	10.102.203.194	10.102.203.172	SIP/SDP	1303	Request: INVITE sip:4173@10.102.203.172:5062;user=phone | , with session descrip
58	14:17:20.496206	10.102.203.194	10.102.203.172	SIP/SDP	1303	Request: INVITE sip:4173@10.102.203.172:5062;user=phone | , with session descrip
107	14:17:25.526119	10.102.203.172	10.102.203.194	SIP/SDP	809	Status: 200 OK | , with session description
108	14:17:25.527281	10.102.203.172	10.102.203.194	SIP/SDP	809	Status: 200 OK | , with session description
109	14:17:25.580562	10.102.203.194	10.102.203.172	SIP	532	Request: ACK sip:4173@10.102.203.172:5062 |
110	14:17:25.581663	10.102.203.194	10.102.203.172	SIP	532	Request: ACK sip:4173@10.102.203.172:5062 |
111	14:17:25.584404	10.102.203.228	10.102.203.172	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x22F8CED0, Seq=42868, Time=586731216
112	14:17:25.587707	10.102.203.228	10.102.203.172	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x22F8CED0, Seq=42868, Time=586731216
113	14:17:25.603805	10.102.203.228	10.102.203.172	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x22F8CED0, Seq=42869, Time=586731376
114	14:17:25.604505	10.102.203.228	10.102.203.172	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x22F8CED0, Seq=42869, Time=586731376

Imagen 1.54 (Wireshark)

Vamos a seleccionar sólo uno de estos flujos:

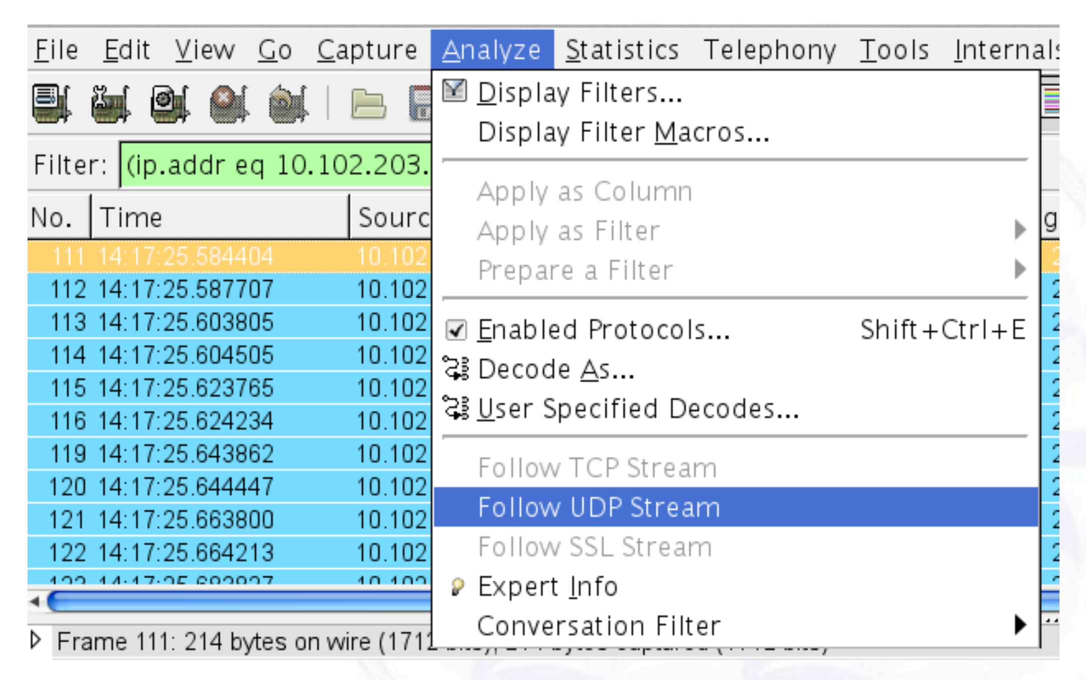


Imagen 1.55 (Wireshark)

Sobre el flujo seleccionado, vamos a analizar el diálogo:

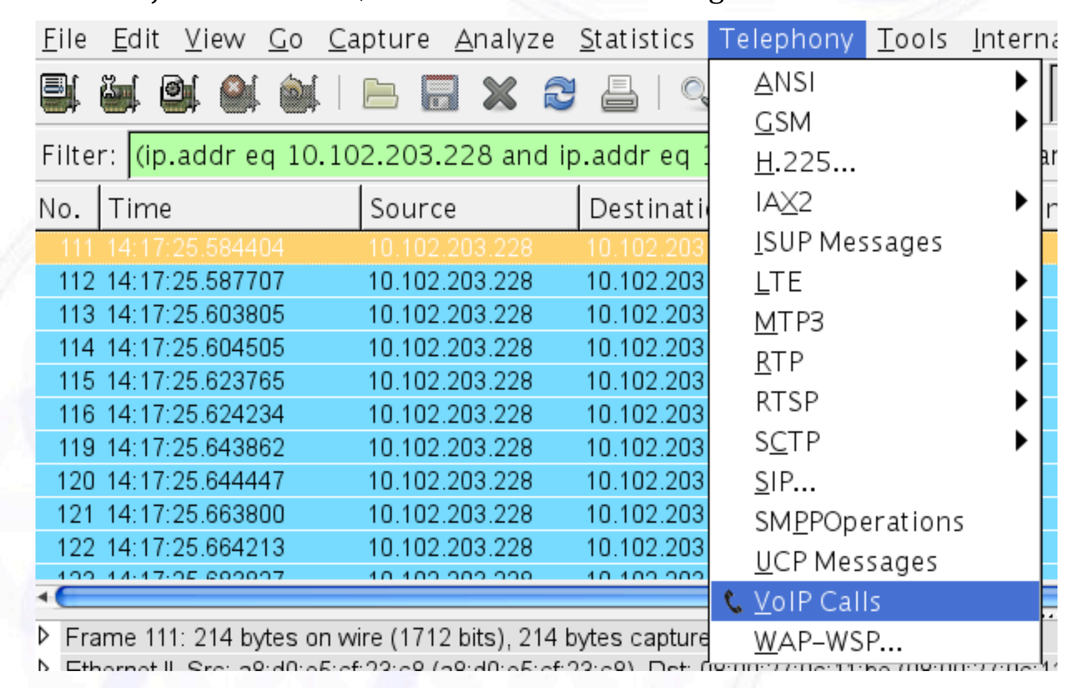


Imagen 1.56 (Wireshark)

Una vez seleccionado el diálogo, debemos decodificarlo:

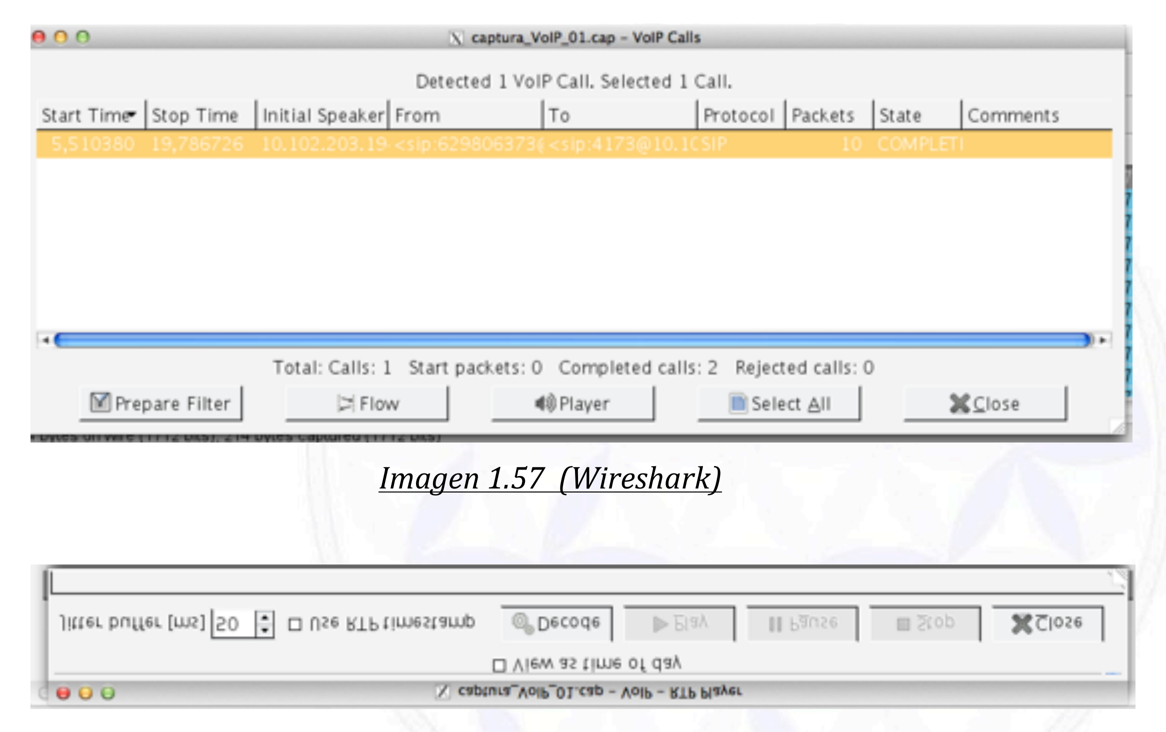


Imagen 1.57 (Wireshark)

Imagen 1.58 (Wireshark)

Por último podemos escuchar el mismo:

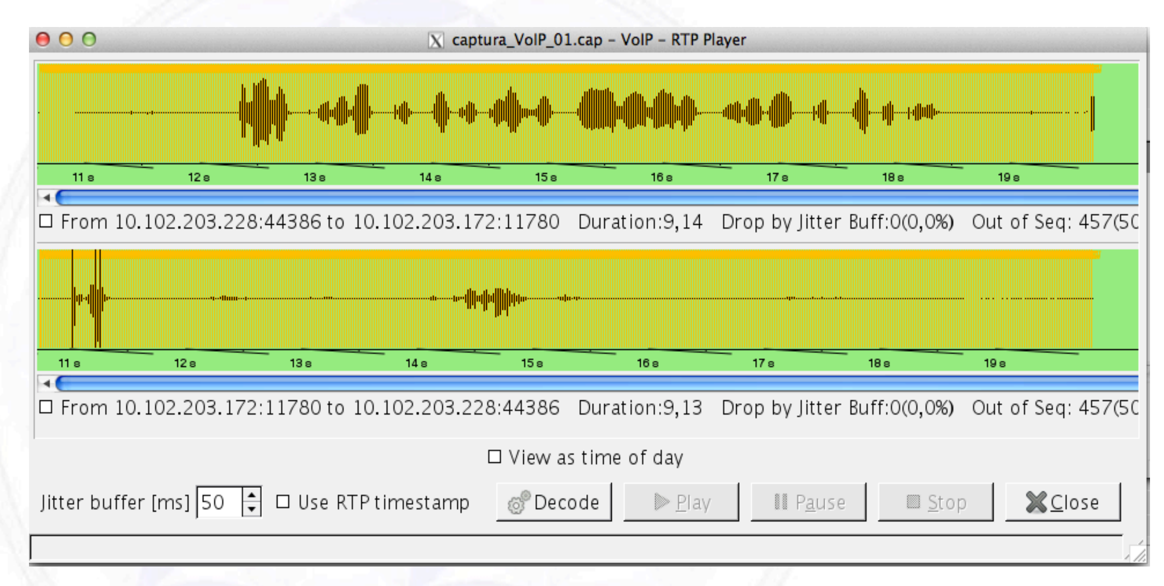


Imagen 1.59 (Wireshark)

Se pueden descargar todas estas capturas de tráfico en www.darFe.es

Se ha intentado presentar de forma resumida, la metodología y las herramientas con las cuáles se puede iniciar este trabajo de investigación y análisis del protocolo SIP.

Lo más importante ahora es comenzar a analizar las RFCs sobre este tema y verificar cuáles de sus postulados pueden abrir puertas no deseadas pero ya no desde el punto de vista de VoIP sino como un protocolo de señalización de grandes redes de telecomunicaciones que es dónde mayor impacto puede ocasionar.

1.8.5. Conclusiones de SIP.

PRIMERA REFLEXIÓN DE SEGURIDAD: Al analizar la seguridad de SIP, debemos tener claro que tiene **una portadora exclusiva** y con su propia IP para este tráfico que no debemos confundir con los caminos de datos o voz.

SEGUNDA REFLEXIÓN DE SEGURIDAD: SIP nace en el UE y llega hasta el P-CSCF (*de forma directa*) pasando por eNB, MME, SGW, PGW, PCRF y HSS…… *Si no se coloca algún dispositivo intermedio*

TERCERA REFLEXIÓN DE SEGURIDAD: El **SBC** es la pieza clave de la Seguridad en VoLTE.

CUARTA REFLEXIÓN DE SEGURIDAD: Se deben emplear los mecanismos de seguridad intrínseca de la RFC-3261 para el empleo de SIP.

Como se ha tratado de presentar durante todo este texto, lo que es verdaderamente importante de SIP no es lo que estamos haciendo hasta ahora centrado en la idea de VoIP. El gran desafío que tenemos por delante va mucho más allá pues en muy pocos años, casi toda la señalización de Internet y de telefonía dependerá de este protocolo, para ello hay cientos o miles de expertos de las grandes corporaciones de telecomunicaciones que están investigando y desarrollando el mismo. Como siempre ha sucedido, los expertos en comunicaciones, conocen al detalle las medidas a adoptar para que esto funcione, no se caiga, tenga latencia mínima, caminos redundantes, control de errores, sea estable a incidencias, etc… pero como siempre ha sucedido también, su "expertiz" no es la seguridad, por lo tanto a medida que van entrando en producción estos nuevos diseños SIEMPRE aparecen problemas de seguridad, pues es normal que así suceda.

El desafío que nos propone SIP es grande, pues como nos lo demuestran las RFCs, se trata de un protocolo muy maduro en su diseño, con más de 160 recomendaciones que lo han ido ajustando, con más de 40 años de experiencia en señalización.

Pero todo esto tiene un importante punto débil:

Es la primera vez en la historia que TODA LA SEÑALIZACIÓN SERÁ POR IP

Y sobre la pila **TCP/IP** **sabemos más que los expertos en señalización**……..

Lo único que debemos tener en cuenta, es que esta diferencia competitiva, para un desafío tan grande implica "hincar los codos" y ponerse a analizar SIP "RFC por RFC". Este debe ser el punto de partida de cualquier línea futura en seguridad.

2. Estrategia de Seguridad en grandes redes

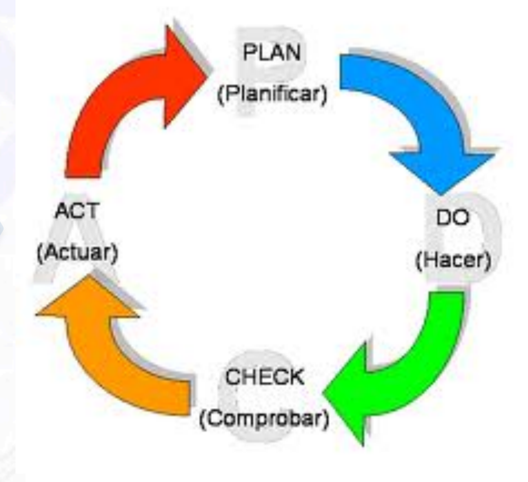
2.1. Organización del área de Seguridad.

Supongamos desde un enfoque **ISO-27000**, que nuestro ámbito de aplicación es: "**arquitectura y gestión de la red de la empresa XXXX**".

Presentaríamos un enfoque de:

a. Valoración de riegos (Risk assesment).
b. SGSI.
c. Controles.
   - Política de seguridad
   - Organización de la información de seguridad
   - Administración de recursos
   - Seguridad de los recursos humanos
   - Seguridad física y del entorno
   - Administración de las comunicaciones y operaciones
   - Control de accesos
   - Adquisición de sistemas de información, desarrollo y mantenimiento
   - Administración de los incidentes de seguridad
   - Administración de la continuidad de negocio
   - Marco legal y buenas prácticas

¿Cómo lo propone ISO-27000?



Para poder organizar un área de Seguridad en Red que responda a la línea propuesta por la familia ISO-27000, lo mejor es tomar como punto de partida un organigrama como el que se presenta a continuación:



El objetivo de esta sección (*como todo el libro*) es proponer una metodología de análisis y evaluación "**Técnica**" de cada uno de estos temas.

2.2. Planificación de la Seguridad.

El **Objetivo** de Planificación, es fundamentalmente "pensar" las diferentes soluciones de Seguridad para que desde el inicio (entrada en producción) de todo dispositivo/plataforma/Infraestructura/software etc.. se consideren sus parámetros de seguridad. Ya todos conocemos el impacto que ocasiona cualquier nueva implantación, cuando está ya funcionando en nuestra empresa y aparece una necesidad de cambio por cualquier factor; en esos casos suele ser un coste mucho (pero mucho) mayor implementar estas modificaciones sobre la marcha que si las mismas fueron pensadas y analizadas desde el principio. Desde el punto de vista de la Seguridad no sólo es una cuestión de coste, sino de Riesgo e Impacto real para todo el resto de la infraestructura de la empresa, pues si es mismo elemento a su vez abrió una brecha de seguridad y la misma fue explotada indebidamente puede ocasionar una pérdida muchísimo más alta.

El Planeamiento debe definir el ciclo de vida de la seguridad (**SGSI:** Sistema de Gestión de la Seguridad de la Información) y diseñar la implementación de las medidas técnicas a aplicar para la mitigación de los riesgos que definió el nivel Estratégico de la organización, adecuándolos a los cursos de acción seleccionados y con los recursos que se asignen a cada uno de ellos.

Una de las actividades más importantes de Planificación de la Seguridad de red es toda la ingeniería de infraestructuras (creación de planta, gestión de cambios, gestión de configuraciones e inventario, etc.) y los procesos que mantienen "viva" la seguridad (Gestión de incidencias, gestión de accesos, gestión de backups, gestión de Logs, supervisión y monitorización, etc), todos estos procesos se verán en detalle en otro capítulo.

Partiendo de estos conceptos es que Planificación de la Seguridad podemos presentarla desde la siguiente imagen:



De cada uno de ellos se desencadenarán una serie de "Sub" procesos que son los que figuran por debajo en la imagen. A continuación desarrollamos todos ellos.

a. Análisis técnico. (Análisis de Viabilidad Técnica):

¿Qué subprocesos contempla?

1) Especificación Técnica de Requisitos funcionales, de Seguridad y de Gestionabilidad.

Es el requerimiento técnico inicial de lo que se desea incorporar.

2) Informe de Análisis Técnico. (funcionalidad, escalabilidad, seguridad).

Es el requerimiento de parámetros técnicos globales de la solución que se desea implantar.

3) DTS (Definición Técnica de la Solución) Red Preliminar.

Es el requerimiento detallado y completo de las funcionalidades, rol dentro de la red, capacidades, etc..

b. Pruebas de Laboratorio.

¿Qué subprocesos contempla?

1) Autorización de **FOA** (First Office Application).
1) Documentación de Integración con sus plataformas de gestión.
2) Descripción técnica de detalle.
3) Documentación de Implantación para FOA.
4) Informe de Pruebas Laboratorio.

c. Pruebas en Red (Realización de las pruebas con tráfico real en primera instalación).

Si todo ha sido correcto los siguientes pasos serán:

1) Autorización de Introducción en planta para Despliegue.
2) Documentación de Despliegue.

3) Informe de Acreditación de Seguridad.
4) Informe de Pruebas FOA.

¿Qué debe conocer planificación?

Lo más importante para Planificación de la Seguridad de red es conocer detalladamente los elementos fundamentales de switching, routing y seguridad de una red.

En la actualidad no existe otra forma de plantearse un diseño de red que no sea por "Capas de Seguridad".

a. Capas (*Defensa en profundidad*).

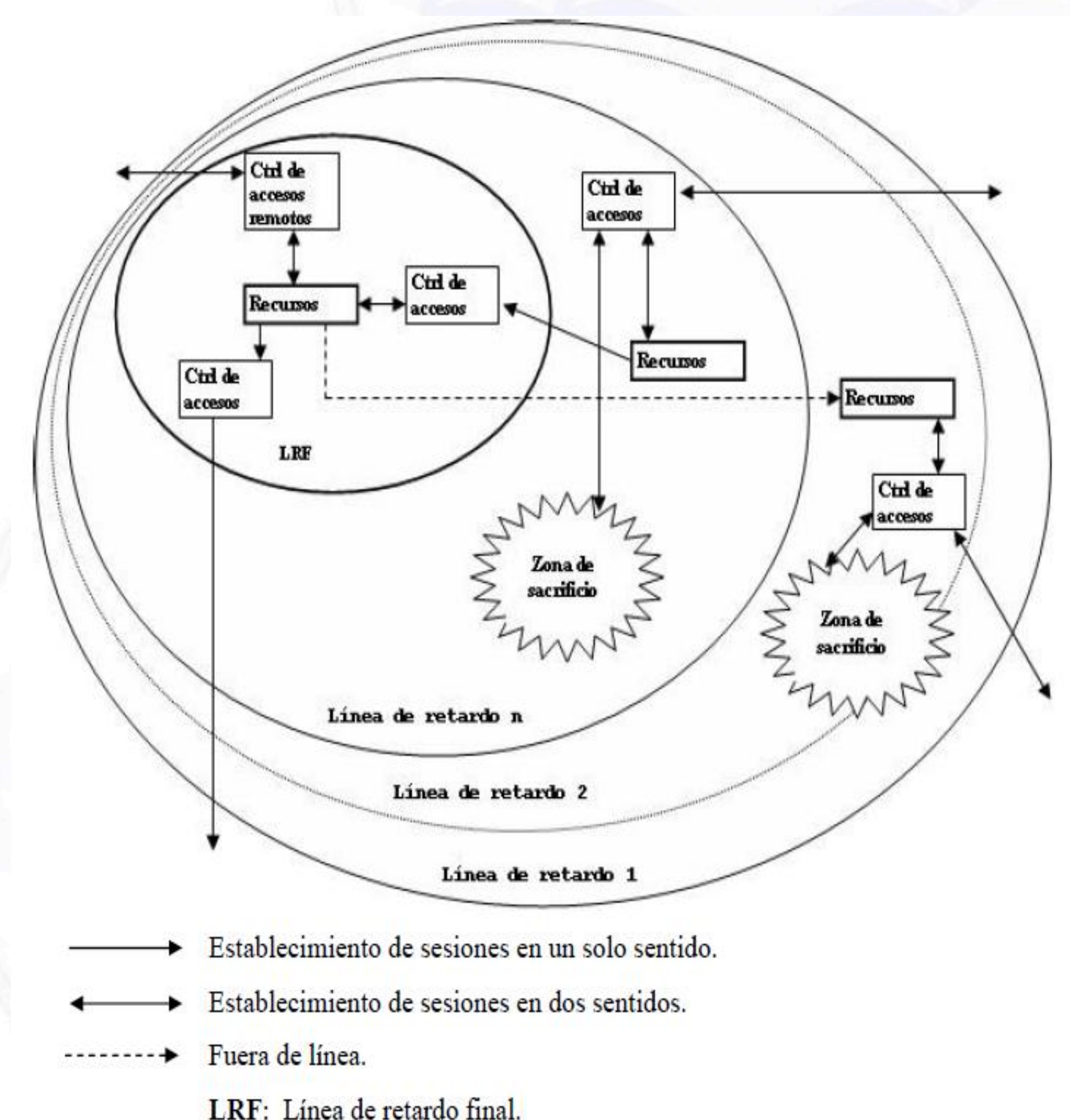


Imagen 2.1 (líneas de defensa en profundidad)

Si esas "capas" las comenzamos a pensar con los elementos que permiten dividir las diferentes zonas o controlar los flujos que por ellas circularán, podemos presentarlas según la imagen que sigue.

b. Componentes por niveles de una red.

Imagen 2.2 (líneas de defensa en profundidad - dispositivos)

2.3. Gobierno de la Seguridad.

El Gobierno de la Seguridad de red es la actividad que mantiene "vivo" el estado de seguridad. Supervisa, audita y diseña las acciones de mejora necesarias para mantener el ciclo. Tampoco merece la pena entrar en detalle sobre esta actividad, pues hoy contamos con la ya mencionada familia ISO-27000 cuyo nombre es justamente **SGSI**, que nos describe con máxima profundidad cómo llevar adelante esta actividad de Gobierno continuo de la seguridad.

Sobre los conceptos de SGSI e ISO 27000, en este texto no nos extenderemos más pues ya ha sido tratado en el libro "**Seguridad por Niveles**"

Sólo mencionaremos que el área de Gobierno es la responsable de este ciclo PDCA, por lo tanto debe contar con herramientas que le permitan "Chequear" (auditar) y generar acciones de mejora para realimentar el ciclo de vida.

Veamos ejemplos de ellas:

- ccsat.
- Nipper-ng.
- Nessus.
- Kali.
- Herramientas de gestión de Firewalls (*Firemon – Algosec – tuffin*)

Guías CIS.

- http://www.cisecurity.org/

2.4. Operación de la Seguridad.

El nivel Operacional es el "**Cómo**" de toda la operación.

Este nivel es el que opera el día a día. Para un Operación de Seguridad de red, no pueden existir improvisaciones, ni despliegues que no cuenten con un marco sólido de Seguridad, sino será comprometida casi con certeza en el corto plazo.

¿Dónde entra Operación? Presentación de niveles de red.

Aplicación	Usuario
Transporte	Es el primer nivel que ve la conexión "de Extremo a Extremo"
Red	Rutas
Enlace	Nodo inmediatamente Adyacente
Físico	Aspectos Mecánicos, físicos y eléctricos (u ópticos)

Desde aquí hacia arriba mira hacia el usuario

Desda aquí hacia abajo mira hacia la Red

¿Qué hace cada uno de ellos? o ¿Qué hace cada elemento de red y en qué nivel?



Switch (Nivel 2) → Conoce el direccionamiento de este nivel (**MAC**).



Access Point (Nivel 2) → Conoce el direccionamiento de este nivel (**MAC**).



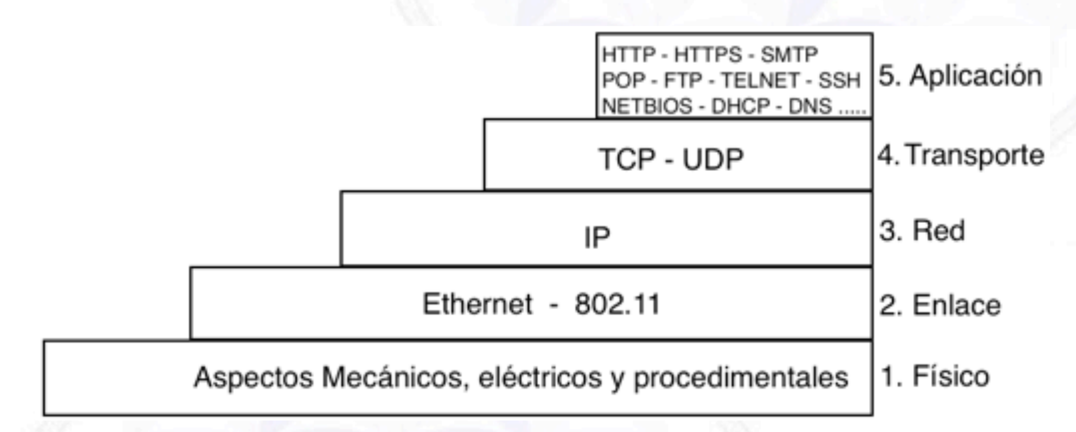
Router (nivel 3) → Conoce el direccionamiento de este nivel (**IP**).



Firewall (varios niveles)→Conoce hasta el nivel de Transporte (**TCP/UDP**)*

(*) También hay FWs de nivel Aplicación (pero no son motivo de esta libro).

Presentación de protocolos básicos de red.



La mejor forma de comprender y analizar cada uno de estos protocolos de red es a través de herramientas que nos permitan visualizar la totalidad de los "bits" que circulan por la misma.

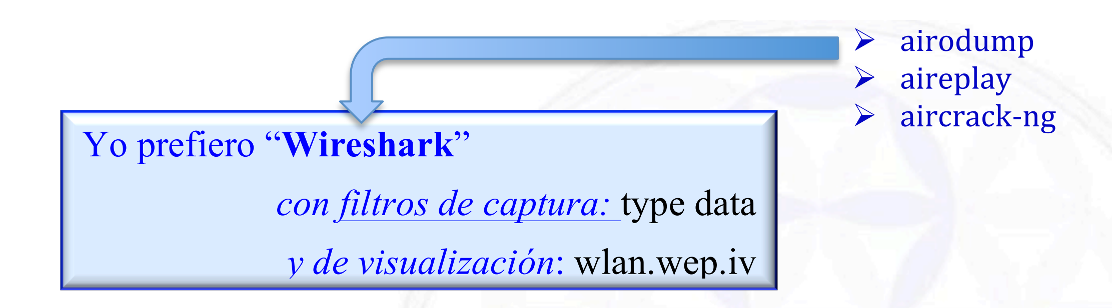
a. ¿Cómo se analizan los niveles? → "**Wireshark**" (ex-Ethereal) o **"tcpdump"**.
b. En particular se debe tener claro la importancia de los protocolos seguros e inseguros de estos niveles.

   Ejemplos (Ver capturas de tráfico desde http://www.darFe.es):

   - Capturas telnet y SSH
   - http y https
   - ftp y sftp

c. ¿Cómo analizo elementos de red? → **nmap (Zenmap).**
d. ¿Cómo analizo redes WiFi? → Suite **"aircrack-ng"**.

   Esta suite, está compuesta por tres programas:



Antes de trabajar con los ejemplos, presentamos de qué se trata o en qué aplica este nivel de enlace:

Nivel 2 (Enlace) → Direccionamiento MAC: Si bien hoy existe hardware que puede operar en este nivel y superiores, para ser estrictos y comprender la teoría que los sustenta, deberíamos centrarnos en la familia IEEE 802.x (*que merece la pena destacar que este valor 802 tiene su origen en que este subcomité de IEEE se creó en el año "**80**" durante el mes "**2**" (febrero)*).

Si bien existen varios más, por nuestra parte los que más nos interesan son los que se presentan a continuación:

IEEE 802.1	*Se presenta más abajo*
IEEE 802.2	Control de enlace lógico
IEEE 802.3	**CSMA / CD (ETHERNET)**
IEEE 802.4	Token bus LAN (Disuelto)
IEEE 802.5	Token ring LAN (Topología en anillo)
IEEE 802.6	Redes de Area Metropolitana (MAN)
IEEE 802.11	**Redes inalámbricas WLAN. (Wi-Fi)**
IEEE 802.15	WPAN (Bluetooth)
IEEE 802.16	Wimax

El **Grupo 802.1** como indicamos al principio, podemos resumirlo en algunas tareas fundamentales:

- Arquitectura e interconexión LAN/MAN.
- Interconexiones de centros de datos.
- Seguridad.
- Gestión global de la red.

¿Qué nos interesa por ahora de ellas? (*más adelante se verá de forma práctica*):

802.1D: Spanning Tree Protocol

802.1Q: Virtual Local Area Networks (VLAN)

802.1x: Autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible RFC 3748 (**EAP**).

802.11i: Su objetivo es la seguridad WiFi. El estándar abarca los protocolos 802.1x, **TKIP** (Temporal Key Integrity Protocol), y **AES** (Advanced Encryption Standard). Se implementa en **WPA2.**

TKIP: o hashing de clave WEP/WPA, incluye mecanismos para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente. Resuelve el problema de reutilización de los Vectores de Inicialización del cifrado WEP.

AES (también conocido como Rijndael), es un esquema de cifrado por bloques adoptado como estándar por el gobierno de EEUU, es uno de los algoritmos más populares usados en criptografía simétrica.

En toda configuración de red WiFi entra en juego la decisión de emplear: Protocolos WEP, WPA o WPA2.

WEP (Wired Equivalent Privacy)

WPA (Wi-Fi Protected Access) es un sistema temporal para proteger las redes inalámbricas creado para corregir las deficiencias de WEP (Wired Equivalent Privacy).

WPA2 (WPA versión 2): Implanta **CCMP** (CCM mode Protocol) (cuyo verdadero nombre es: Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol). Es el protocolo que marca la diferencia con WPA y es el aporte definitivo de IEEE 802.11i

Todos estos temas de nivel 2 los desarrollaremos de forma práctica en el capítulo de "**Switching**"

Las herramientas básicas que deben operarse, al menos son:

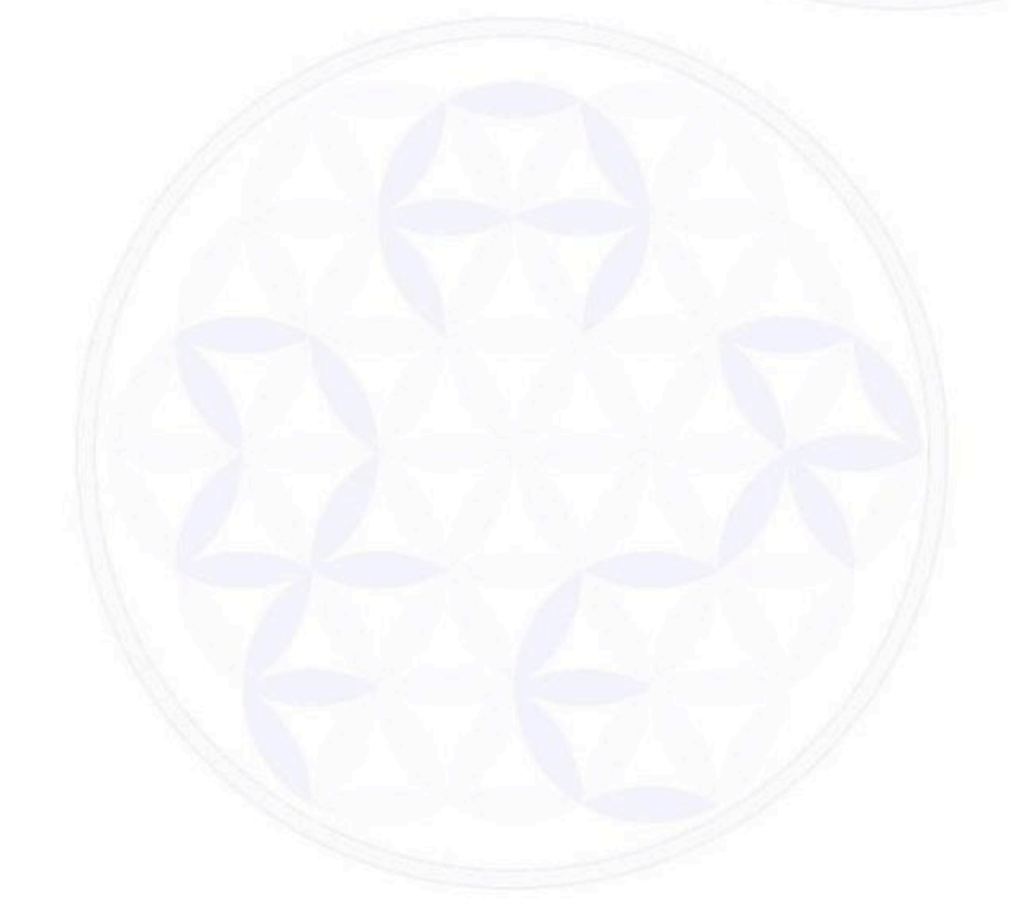
- Herramientas de mitigación de ataques DDoS tipo TMS/Peak Flow de Arbor
- Herramientas de centralización y correlación de Logs (SIEM: *Security Information and Event Management*) del tipo:
  - ArcSight de HP
  - RSA Security Analytics

- Splunk (*Puede discutirse si es o no un SIEM…*)

- Firewalls. En el mercado existen cientos
- Herramientas de gestión de Firewalls del tipo:
  - Algosec
  - Tuffin
  - Firemon
- Herramientas de detección y prevención de intrusiones del tipo:
  - Snort
  - Check Point Intrusion Prevention System
  - Cisco Next Generation IPS
  - McAfee Network Security Platform
  - Se pueden considerar aquí los FWs de nueva generación de Palo Alto
- Herramientas de monitorización y supervisión de red. Dentro de este rubro existen cientos de herramientas, en general fuertemente orientadas a líneas de productos, pero lo que debe interesarnos aquí es que las que se seleccionen debe operar con protocolos estandarizados dentro de las familias de *snmp, syslog, mrtg, etc*.
- Herramientas de gestión de ticketing (también existen varias). Este punto aunque parezca trivial no lo es, ya que todo el control de infraestructuras, dispositivos, redes, etc. Debe responder a una metodología estricta y segura de seguimiento, desde que se da de alta un elemento, se realiza cualquier cambio, se sufre una incidencia, se solicita soporte técnico, se crea o modifica una regla en un FW o IDS, etc. Para cualquiera de estas tareas, es fundamental poseer todo su ciclo de vida (o histórico) pues la actividad de "forense" y la "trazabilidad" serán uno de los pilares de una infraestructura de defensa de red.
- Herramientas de control de acceso, tipo:
  - ACS de Cisco
  - Series SRC de Juniper
  - NAKINA
  - Access Control de Fortinet
  - HPNA
  - CITRIX
- Metodología estricta de sincronización de tiempos basada en el protocolo ntp.
- NOC (Network Operation Center) 24x7

- SOC (Security Operation Center) 24x7
- Infraestructura de telecomunicaciones eficiente y flexible.

De todos los protocolos mencionados, también podemos descargar varias capturas de tráfico de la familia **IEEE 802.xx** desde http://www.darFe.es



3. Procesos de seguridad en redes

Antes de comenzar a desarrollar este tema, vamos a considerara una palabra clave:

"ACIDA"

Desde el punto de vista de la seguridad, y en particular en los procesos, debemos tener permanentemente presente que la seguridad está basada en los pilares o principios de esta palabra clave:

- **Autenticación**: Garantizar que "es quien dice ser"
- **Confidencialidad**: Garantizar que a los datos y a los sistemas solo accedan personas debidamente autorizadas.
- **Integridad**: Garantizar la exactitud de la información y de los sistemas contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- **Disponibilidad**: Garantizar que la información y los sistemas pueden ser utilizados en la forma y tiempo requeridos
- **Auditabilidad**: (También llamado "Trazabilidad") Garantizar que cualquier acción o transacción pueda ser relacionada unívocamente asegurando el cumplimiento de controles claves establecidos en las correspondientes normativas.

Si queremos ir un poco más allá todavía podemos definir también **Control de Accesos**: cuyo objetivo es derivar a cada uno exclusivamente al sitio al cual está autorizado a ingresar (*Por esta razón en muchos textos va a asociado a "Autenticación"*), en muchos textos también, este concepto lo encontraremos relacionado a la última "A" de ACIDA como "Accesos", también esta misma letra algunos la presentan como "Accounting", en definitiva quedémonos con estas ideas, pues son las que darán origen a los procesos que analizaremos en este punto.

Los procesos pueden parecer poco interesantes para alguien que desea dedicarse a la Seguridad en Redes, pero nuestra experiencia al respecto es que juegan un rol fundamental en toda organización de la Seguridad, pues son los que verdaderamente regulan "qué se puede y que no se puede hacer", sin ellos cualquier persona deja librada a su criterio personal y aislado las diferentes medidas, acciones, decisiones, permisos, rutas, reglas, borrados, cambios, procederes, reacciones…… cualquiera de estas palabras suenan a ¡*Peligro*! En alguien que se dedique a estos temas.

A lo largo de estos últimos años, hemos tenido la posibilidad de auditar un importante número de redes y también a realizar el seguimiento y retesting de las mismas, lo que más nos llamó la atención es justamente que gracias a haber hecho un fuerte hincapié en estos procesos se ha manifestado un cambio radical en todas ellas. Por esta razón es que si bien somos conscientes que existen muchos más procesos de los que aquí presentamos, hemos seleccionado **específicamente estos ocho** pues son los que cobran una importancia básica en la Seguridad de redes.

3.1. Entrada en producción.

La idea del procedimiento de Entrada en producción, es el conjunto de pasos a seguir desde que un dispositivo, plataforma o servicio es "imaginado", pensado o planificado hasta que el mismo entra en producción.

Para desarrollar este punto tomaremos como referencia un flujo concreto y real de que responde al completo con este proceso. Lo desarrollaremos de acuerdo a los pasos principales que se deben llevar a cabo desde el punto de vista de la Seguridad:

Básicamente se deben considerar tres procesos:

a. Análisis técnico.
b. Pruebas de Laboratorio.
c. Pruebas en Red.

De cada uno de ellos se desencadenarán una serie de "Sub" procesos. A continuación desarrollamos todos ellos.

a. Análisis técnico.

Consiste en preparar y definir todo el detalle posible sobre la arquitectura funcional de la solución pensada para la red, el modelo de escalabilidad, seguridad y las características de integración en todos los ámbitos para realizar su Validación Técnica.

Implica:

- Realizar el análisis de viabilidad.
- Realizar la Definición Tecnológica de la Solución de Red preliminar.
- Evaluar el coste económico si hubiere trabajos externos de desarrollo e integración.
- Acordar la planificación general.
- Realizar las especificaciones, su valoración técnica y elaborar propuestas de selección (si participarán proveedores).

¿Qué subprocesos debe contemplar?

1) Especificación Técnica de Requisitos funcionales, de Seguridad y de Gestionabilidad (*Funcionalidad, Escalabilidad, Integración, Características medioambientales, de transmisión y mecánicas, Equipamiento de maqueta, Soporte técnico, Plan de formación en Seguridad*).

2) Informe de Análisis Técnico. Se trata de información sobre las características técnicas generales de los productos y soluciones de red.
3) Definición Técnica de la Solución. Recoge la descripción general de la solución técnica a implantar. Debería incorporar la siguiente información:
   - Características Técnicas Generales.
   - Características ambientales, de transmisión y mecánicos.
   - Características de Integración.
   - Seguridad.
   - Estrategia de Respaldo.
   - Equipamiento de maqueta para validación.

b. Pruebas de Laboratorio.

Estas pruebas consisten en:

- Analizar y verificar, mediante pruebas en laboratorio las características funcionales, de escalabilidad y/o de integración de las soluciones tecnológicas.
- Obtener la comparativa técnica necesaria para los procesos de selección y compra de soluciones tecnológicas.

Implica:

- Definición del escenario de maqueta para la validación de la solución.
- Elaboración de los documentos de configuración y provisión para la integración.
- Elaboración y realización de los planes de pruebas.
- Participación y colaboración en la integración en maqueta con los sistemas de gestión y configuración.
- Participación en la validación de extremo a extremo.

¿Qué subprocesos contempla?

1) Autorización de la instalación en laboratorio de un determinado sistema/equipo/elemento para la realización de pruebas en un entorno similar al de producción.

2) Documentación de Integración con Sistemas de gestión.
Documento que describe las características de integración en los sistemas de gestión y provisión. Sirve de entrada para establecer las previsiones de disponibilidad y para el inicio de los trabajos de desarrollo necesarios.

3) Documentación de Implantación en laboratorio. Debe contener la siguiente información:

- Control hardware/software.
- Criterios de implantación.
- Pruebas de roll back (vuelta atrás).
- Procedimiento de roll back.
- Escenario y Plan de Pruebas de laboratorio.

4) Informe de Pruebas Laboratorio. Documento en el que, como resultado de un proceso de pruebas se recoge:
    - Escenarios de evaluación.
    - Plan de pruebas y resultados.
    - Recomendaciones u objeciones encontradas, nivel y motivo.
    - Análisis de las diferentes alternativas técnicas disponibles para los escenario.
    - Conclusiones/Valoración técnica.
    - aspectos de seguridad.

c. <u>Pruebas en Red</u> (**FOA**: First Office Application - Realización de las pruebas con tráfico real en primera instalación).

   Una FOA es una primera implantación en la red previa al despliegue en planta. Su función es la verificación del correcto funcionamiento de la solución tecnológica en un entorno de tráfico real e integrada con otros sistemas y redes..

   Si el resultado de la FOA es correcto, las salidas serán:

   - Autorización introducción en planta para despliegue.

   - Documentación de Despliegue.

   Si el resultado de la FOA no es correcto se volverá al subproceso de "Pruebas de Laboratorio" y en caso de ser necesario se enviará a las áreas implicadas en informe de resultados de las pruebas de FOA.

Si **todo** ha sido correcto los siguientes pasos serán:

a) Autorización de Introducción en planta para Despliegue.

   Autorización, de manera condicionada, del despliegue en planta de un determinado sistema/equipo/elemento que, aún pudiendo haber manifestado

ciertos reparos durante las pruebas en laboratorio y/o período de FOA, éstos no impiden su despliegue en red, con el visto bueno del área de seguridad.

b) Documentación de Despliegue.

Incorpora, en caso de ser de aplicación, la siguiente información:

- Metodología final de implantación-marcha atrás.
- Definición Tecnológica de la Solución de Red versión final.
- Procedimiento de Instalación.
- Control Software-Hardware.
- Control de Reparos y limitaciones.
- Informe de acreditación de Seguridad.

c) Informe de Acreditación de Seguridad.
Documento que recoge los riesgos residuales de seguridad y los puntos de no conformidad normativa interna o regulatoria. Los riesgos residuales son aquellas vulnerabilidades conocidas y no resueltas en el proyecto por limitaciones de la tecnología o por restricciones de coste o tiempo de desarrollo.

d) Informe de Pruebas FOA.
Documento en el que, como resultado del proceso de monitorización y pruebas en planta se recoge cuando sea de aplicación la siguiente información:

- Escenarios de evaluación.
- Plan de pruebas y resultados.
- Reparos encontrados, nivel y motivo.
- Conclusiones/Valoración técnica.
- Valoración de seguridad.

En resumen: El objetivo desde nuestro punto de vista, es corroborar que la seguridad está insertada o interviene en cada uno de los sub-procesos, y que se está dando cumplimiento estricto a estos pasos.

Una de las mayores dificultades que se han detectado siempre en las grandes redes, es justamente los problemas técnicos y económicos que implican "pensar" en seguridad recién cuando la plataforma está entrando en producción, o pero aún ya en funcionamiento. En esos momentos cualquier tipo de modificación implica esfuerzos considerables (y hasta a veces inabordables de llevar a cabo).

3.2. Gestión de cambios.

El detalle relevante de este proceso es que hemos podido verificar en reiteradas oportunidades que las incidencias de alto impacto en las redes, se producen por errores, o ausencia de un procedimiento estricto de "control de cambios". Debido a ello, el proveedor o empleado, ha accedido a un dispositivo o plataforma, por ejemplo: en ventanas de tiempo críticas, con escalado de privilegios, con usuarios genéricos, en zonas restringidas, ejecutando comandos que no debía, por accesos – vínculos - enlaces o plataformas no autorizados, sin dejar "Logs" de su actividad, excediendo los permisos que tenía para realizar una determinada actividad, etc. Y con ello se han sufrido caídas de horas (e inclusive días) en servicios críticos (DNSs, Servidores, Switchs y Routers de Core….)

El principal objetivo del proceso de control de cambios es que paulatinamente se esté intentando, paso a paso, ajustar al máximo estos detalles. Nuestra experiencia es que en general, se trata de un proceso que aún en las grandes redes, no se le ha dado la importancia que merece. Nuestro objetivo final, y hacia donde deberíamos apuntar sin lugar a dudas es:

1) Proceso de Gestión de cambios.
2) Integración con Gestión de usuarios.
3) Integración con alguna metodología de Identity Manager.
4) Integración con Workflow de seguimiento.
5) Integración con Gestión de incidencias.
6) Integración con proceso de "autenticación" o "Control de accesos"

¿Qué es lo que tratamos de transmitir en estas líneas?:

- Todo usuario debería tener un identificar único que le permite acceder a las plataformas o dispositivos de su responsabilidad.
- Se debe mantener "vivo" el ciclo de vida de usuarios.
- Cada usuario debe poseer determinados "roles o perfiles" permanentes (deberían ser mínimos y escalables en determinados intervalos de tiempo), pueden existir (contados y claramente identificados) un muy reducido grupo de usuarios con alto nivel de privilegios (verdaderos especialistas del tema, y son los únicos que sí pueden ejecutar comandos críticos).
- Los accesos deben estar claramente definidos y controlados.
- Las tareas de mantenimiento o cambios deben ser: Programadas (la mayoría) y algunas No Programadas (bajo mayor control).
- Para las tareas programadas, se configuran "ventanas de tiempo" en horarios de baja criticidad, y exclusivamente en estas ventanas se eleva el

privilegio del usuario que haya sido autorizado, finalizada la ventana, esos privilegios se pierden.

- El NOC, a través del Workflow correspondiente, se debe mantener alertado durante todo el proceso.
- Se deben poseer todos los mecanismos adecuados de alarma y escalado de incidencias.
- Se debe mantener todo el ciclo de trazabilidad de la actividad.
- Debe existir un "Comité de Gestión de cambios" (*actas, integrantes, frecuencia reuniones, seguimiento de: informes, estadísticas, mejoras*)
- Debe existir un "Flujo" de aprobación de cambios.
- Es fundamental emplear "Escalabilidad de privilegios", siendo por defecto únicamente el acceso de lectura.
- Monitorización de la actividad
- De los cambios críticos deben surgir informes, estadísticas, acciones de mejora.

3.3. Gestión de accesos.

Lo más importante a considerar para la "Gestión de accesos" es tener la capacidad de derivar a cada uno exactamente dónde debe acceder. Ni a más, ni tampoco a menos dispositivos/servicios/redes/aplicaciones/funciones que las que le corresponde).

La gestión de los dispositivos de red, es una actividad que debe ofrecer disponibilidad y redundancia máxima para poder llegar y conectarse a los diferentes elementos ante cualquier anomalía o para tareas habituales de administración, pero no por ello desde el punto de vista de la seguridad, debemos emplear "reglas holgadas" para que todo el mundo pueda hacerlo, sino todo lo contrario. No es sencillo, pero sí es muy importante poder garantizar que "solo accede quien debe hacerlo y con los privilegios que necesita".

Las ideas fuerza con la que nos deberíamos quedar en cuanto al funcionamiento de esta actividad son:

1) Qué exista y se cumpla un documento "Control de accesos".
2) Deben estar definidos los pasos para la solicitud, administración y anulación de los derechos de acceso.
3) Debe existir el rol de "Gestor de usuarios", y esta persona (o área) mantendrá actualizado "registro y gestión de identidades".
4) Debe establecerse y llevarse a la práctica el Ciclo de vida de las cuentas de usuarios.

5) Es importante el empleo de herramientas de workflow para control de accesos para poder tener una trazabilidad completa de los mismos.

6) Debe estar documentado y definido un perfilado de usuarios para los diferentes accesos (Lectura / Mantenimiento estándar / Mantenimiento avanzado/ Administrador, etc.)

7) De ser posible debería estar integrado con AD, LDAP, RRHH, etc..

8) Se debe hacer todo el esfuerzo posible para eliminar las cuentas genéricas y locales en los dispositivos.

9) Debe se riguroso el empleo de diferentes "Privilegios" de acuerdo al nivel de acceso.

10) Se deben emplear siempre "Ventanas de acceso" cuando se realicen actividades que pueden ser críticas para la estabilidad de la red.

11) Se debe incrementar al máximo el concepto de "Granularidad" para el acceso a los diferentes dispositivos. (elemento, red, plataforma, proveedor).

12) Es fundamental implementar "Plataformas de trazabilidad de accesos", que permitan realizar cualquier tipo de análisis sobre el ciclo histórico de accesos.

13) Una de las actividades básicas de cualquier intruso es la evasión de los controles de acceso, por lo tanto debe ser implementadas "Medidas de control" sobre potencial evasión del control de acceso.

Veremos más adelante que para la gestión de accesos, es de suma importancia el concepto de "Segmentación de redes", en particular lo que definiremos como "Redes de Gestión". Para poder asegurar que las configuraciones de nuestros elementos de red cumplan con los requisitos de seguridad establecidos, una de las reglas básicas es poder diferenciar bien diferentes zonas desde las cuales la "visibilidad y funciones" de los dispositivos responden de forma diferente, un ejemplo básico lo podemos ver en un servidor Web:

- Si accedo al mismo por ejemplo desde Internet, podríamos plantearlo como que lo hago desde una zona desmilitarizada (o DMZ) para que me ofrezca un "servicio" que podría ser hacia cualquier usuario desconocido.
- Si accedo al mismo desde dentro de mi empresa, en este caso podríamos pensarlo como una "Intranet", accediendo únicamente los empleados de la empresa.
- Si ese servidor Web, realiza una consulta hacia una base de datos de la empresa, la misma estará en una zona militarizada (o MZ) con un nivel de seguridad más estricto.
- Si a ese servidor se conectara su administrador para tareas de gestión, debería hacerlo desde una "red de Gestión" a la que solo acceden los administradores de red.

En resumen acabamos de ver que a ese dispositivo se puede acceder desde: Internet, Intranet, MZ y red de gestión. Si somos capaces de "Segmentar" adecuadamente cada una de ellas (como veremos más adelante) colocando diferentes barreras, controles y supervisión sobre las mismas, podemos afirmar que hemos incrementado el control de accesos de estos segmentos de red, elevándolo a un nivel de seguridad mejor que si no lo hiciéramos.

3.4. Configuraciones e inventario.

Cuando hablamos de seguridad, es imposible adoptar medidas o tomar decisiones si no sé qué es lo que debo asegurar. Ninguna empresa de seguros me otorgaría una póliza sin saber qué es lo que está asegurando, ninguna empresa de vigilancia podría prestar servicio si no supiera qué debe vigilar….. en una red es exactamente igual. Es imposible abrir una regla en un Firewall si no se conoce en detalle la comunicación de extremo a extremo que se está habilitando, no se puede lanzar un plan de continuidad de negocio si no se sabe con que recursos se cuenta, no se puede crear una VLAN (Virtual LAN) si no se sabe cuáles son los elementos que la deben integrar. Podríamos seguir citando cientos de ejemplos más, pero cualquier tipo de análisis de seguridad que se desee realizar necesita contar con el máximo nivel de detalle sobre las configuraciones e inventario sobre el que se va trabajar.

Aunque sea una verdad irrefutable, en general no suele ser así. Es cierto que en un gran red, es muy difícil mantener actualizada la planta y las configuraciones de cada elemento pues la dinámica actual es muy grande, pero no por ello se deben bajar los brazos, pues unas de las consecuencias más frecuentes que produce este hecho es justamente la integración de un dispositivo que "cortocircuita" niveles de seguridad, reglas de Firewall que abren puertas traseras, puertos que quedan expuestos, diferencias en los niveles de bastionado (o hardening) entre dispositivos similares en los mismos segmentos de seguridad (que luego son aprovechados con mala intención), diferencias de parcheado, dispositivos obsoletos que quedan fuera de control, etc.

Cualquiera de estos errores va a suceder "sí o sí" en la medida que comencemos a abandonar el inventario de nuestra red.

El inventario de activos debe ser lo más completo posible (descripción del activo, propietario del activo, encargado del tratamiento del activo, nivel de criticidad, etc.)."

¿Cuáles son los aspectos más importantes que debemos considerara al respecto?:

1) Procedimiento de configuraciones y gestión de inventario: Redacción, aprobación y existencia del procedimiento.
2) Alcance del procedimiento (áreas a las que aplica y las que no): ¿Es adecuada la implementación de estos procedimientos?, ¿abarca toda la organización?

3) Detalle del nivel alcanzado (Hitos a cumplir, importancia de campos, flujos de alta, modificación y baja de datos, metodología de actualización y mantenimiento, parches y obsolescencia, responsables de los datos, etc.). Se trata aquí de evaluar la profundidad y el nivel de detalle de este procedimiento. En general suele existir una gran debilidad en cuanto al mantenimiento de los mismos. En pocas redes se poseen herramientas más o menos automatizadas que ayuden a la actualización de los mismos, a su vez se podría afirmar que casi en ninguna existe un inventario centralizado que esté verdaderamente "vivo" y que facilite una información global de los elementos de red de la misma.
4) Integración de este proceso con los de "Entrada en Producción" y "Control de cambios" pues es la única forma de mantener "vivo" el mismo.

Desde el punto de vista de la seguridad, esta tarea debería ser tomada en cuenta con máxima rigurosidad, pues gran parte de las debilidades que son aprovechadas se deben a descubrimiento de fallos en plataformas, dispositivos o software; cuando a través de la red comienza a difundirse esta información, la búsqueda con malas intenciones crece exponencialmente. La mejor solución y respuesta a este tipo de problemas es poder tomar medidas rápidas al respecto, para ello no cabe duda que lo más eficiente es identificar la totalidad de elementos de red que son de ese fabricante, modelo, software, versión etc… y el sitio natural donde buscarlo es justamente en este inventario.

Una muy buena práctica que deseamos destacar aquí es la implantación de un mecanismo de <u>control de obsolescencia</u> con los diferentes proveedores, y bajo el cual, periódica y obligatoriamente se va recibiendo la información de las versiones a actualizar, parches a instalar, dispositivos que deberían ser cambiados, módulos, etc. La misma se ingresa al inventario y desde allí se pueden generar reportes, alarmas, acciones, etc.

El último aspecto a considerar también desde el enfoque de seguridad, es el de autenticación y control de accesos a la información de este inventario, pues es un repositorio de información vital para la red, cualquier persona no autorizada que obtenga estos datos ya tendría una importantísima base de conocimiento para poder trabajar en nuestras redes y sistemas.

Dentro de este proceso cuando la documentación se mantiene actualizada y "viva" no podemos dejar de lado las arquitecturas que se implantan en las diferentes redes, y como van cambiando a medida que se "inventaríen" altas, bajas cambios o modificaciones. En este punto pondremos de manifiesto que es lo que nos interesa verificar de forma práctica sobre este tema.

<u>Planos modelo de red</u>.

Cuando nos referimos a plano modelo, lo que intentamos expresar es un mapa que contemple con la máxima claridad el modelo "GLOBAL" de la arquitectura, y desde el punto de vista de red *(es decir identificando este nivel del modelo*). Veremos que es posible que esto se cumpla o no en determinadas áreas de la empresa, en realidad está bastante generalizada la existencia de estos planos. El problema radica cuando los mismos:

- Son de uso exclusivo de esa área (o peor aún: persona).
- Responden a un modelo que sólo se entiende en esa área.
- No comprende, ni identifica sus fronteras, interfaces, vínculos de conexión con el resto.
- No responde a un procedimiento Global.
- No representa el nivel de red.

Existen un sinnúmero de situaciones en las cuales la visión global clara y unívoca de estos mapas es de suma importancia, y cuando no existen, abren posibilidades de errores de seguridad, por ejemplo:

- Al configurar reglas en un Firewall.
- Al configurar ACLs en routers y/o switchs.
- Al configurar rutas (estáticas, próximo saltos, pesos, políticas, salto por salto, etc).
- Al configurara VLANs.
- Al habilitar permisos de acceso a dispositivos con parámetros avanzados.
- Al configurar IDSs/IPSs/IDPs/Honey Pots.
- Al determinar acciones AntiDDoS, patrones de Spam, o antivirus de red.

Por lo tanto, el objetivo que deseamos presentar en este control, es considerar los siguientes aspectos:

- Área responsable.

  ¿Existe personal dedicado a esta tarea?, ¿Disponen del tiempo y los acuerdos para mantener vivo el mismo?
- Recursos asignados

  ¿Poseen los recursos necesarios? (Tanto materiales como humanos)
- Alcance (nivel de centralización)

  ¿Qué porcentaje de la red total de la organización cubren estos inventarios?, ¿Se encuentran centralizados en un área específica, o en diferentes?
- Nivel de detalle.

  ¿Es suficiente el detalle de los mismos?

Cuáles son los aspectos básicos:

- Nombre y direcciones IP (de todas sus interfaces, en lo posible con aclaración de qué se trata cada una de ellas).
- Función
- Nivel de criticidad
- Propietario del activo y encargados.
- Ubicación física (de ser posible con máximo detalle: Sala, rack, puertos del switch, cableado, etc.)
- Red o subred a la que corresponden sus interfaces
- Sistema Operativo (de ser posible con su fecha de entrada en producción, actualizaciones históricas y el ciclo de obsolescencia del proveedor.
- Aplicaciones instaladas.
- Control de cambios.
- Registro de incidencias

- Herramientas que emplea
- Qué tipo de herramientas emplea?, ¿Son adecuadas, suficientes?, ¿Responden a todas las necesidades de la red?, ¿Ofrecen mecanismos seguros de autenticación y control de acceso?
- Nivel de actualización de datos.

  Este control debe ser eminentemente técnico, y verificando que verdaderamente queda reflejada la realidad de la planta instalada, es decir se deben realizar pruebas de conexión a diferentes dispositivos, y corroborar lo inventariado con los elementos en producción.
- Metodología de mantenimiento (alta, baja, actualizaciones).

  ¿Es adecuada esta metodología?, ¿Se aplica como debería?, ¿Es real lo establecido con lo que se aprecia en los dispositivos?, ¿Posee algún tipo de mecanismo de automatización o relevamiento de los cambios o nuevos elementos?
- Permisos de acceso a la información.

  Este es un tema que se ha presentado como "conflictivo" pues obtener la información de un inventario de red para un intruso es valiosísimo, pero por otro lado, esta información debe ser de fácil acceso (para consulta y/o modificación) de quien verdaderamente lo necesite, por lo tanto las medidas de seguridad sobre los inventarios, deben ser meticulosas y monitorizadas al detalle, para poder encontrar el justo equilibrio.

  Se han detectado casi siempre problemas justamente sobre este equilibrio en varias redes, por lo tanto, se aconseja evaluar esta actividad a lo largo de toda la revisión de seguridad, verificando

constantemente las áreas que tienen acceso, las que no, las posibilidades de acceder a esta información desde diferentes sitios físicos, las medidas de seguridad de los responsables del dato y de los responsables de la plataforma, etc.

¿Qué necesitamos de los planos?

- Los planos deben estar accesibles a toda persona que los necesite (de esa área o del que fuera), y a su vez restringido en detalle a quien no deba verlos.
- Los planos deben reflejar la arquitectura a nivel red, es decir su esquema de direccionamiento IP, con las máscaras correspondientes para delimitar dónde comienza y finaliza cada segmento de red.
- Para cada dispositivo deben estar identificadas todas sus interfaces activas, pues no nos sirve de nada evaluar toda la red, si luego aparecen nuevas conexiones que no se tuvieron en cuenta.
- Debe quedar legible el nombre de cada nodo (y de ser posible su función).
- De ser posible, se puede aclarar la identificación de esa interfaz física o lógica (Gi1, Eth0/1/0.234, Con1, Internet, Empresa A,B, etc.).
- Cuando existan fronteras que no entran en ese plano concreto, se debe dejar una referencia acerca de dónde y cómo identificar el plano que le sigue a este.
- El empleo del concepto de "capas" en los actuales software de diseño, es sumamente útil para sumar las capas que se necesiten a la hora de cualquier tipo de análisis, dejando fuera las que en ese momento no interesen, pero que sí existen y se pueden mostrar con sólo "habilitar" esa capa concreta.

Buenas y malas prácticas

- La mejor práctica que hemos observado es la integración de:

Inventarios y planos bajo la supervisión de un área concreta para ello.

y

Su inclusión en los procesos de "Gestión de cambios" y "Creación de planta"

- El empleo de herramientas "semi" automatizadas para la gestión de planos e inventario.
- La centralización de los mismos.

- La definición de un modelo de datos, abreviaturas e imágenes única para toda la organización.
- La peor práctica es la ausencia de los mismos, seguida de áreas independientes donde cada uno lleva este tipo de información aislada y sin compartirla.

Confrontación de planos con realidad (¿Cómo analizar estas diferencias?)

Esta actividad ha sido tal vez una de las mayores sorpresas que nos hemos llevado en la confrontación de lo escrito con la realidad. Ha sucedido en muchos casos, que iniciamos la visita de seguridad en una red, con el estudio de planos previos que se nos habían enviado, luego el área de "Planificación y/o Ingeniería" ya "in situ" nos daba una explicación que en algunas oportunidades ya ponía de manifiesto que los planos no eran tal cuál funcionaba la empresa, y por último al irnos conectando a los diferentes dispositivos y evaluar sus configuraciones, se hacía evidente que la realidad no guardaba relación con lo escrito.

Aquí es donde aporta un gran valor agregado el conocimiento de "herramientas de análisis de tráfico", pues a través de ellas se comienzan a evidenciar flujos que deben o no estar presentes sobre esa arquitectura en concreto, por esa razón es que las consideramos como muy importantes en nuestra labor, y finalmente serán la evidencia de que el proceso no está aplicando en la realidad.

3.5. Gestión de Backup.

En general, se nota una gran diferencia entre el nivel de concienciación que tiene el perfil de personal de TI, respecto a la gente de red. Cabe señalar que los dispositivos de red, poseen mucha más estabilidad que los de TI (aplicaciones, desarrollos, programas, BBDD, etc), también es cierto que existen muchísimos menos virus y troyanos para dispositivos de red que para los de sistemas, se suele hacer evidente que el personal no le presta el mismo grado de atención al resguardo y recuperación de sus configuraciones y Logs, es frecuente escuchar "… pero es que este dispositivo no se ha caído nunca en sus años de servicio…." Y en muchos casos es cierto, pero también en muchos otros no. Por esta razón es que creemos que es casi una obligación comenzar a despertar conciencia sobre la importancia de las copias de respaldo y también de sus procesos y pruebas de recuperación.

Otro inconveniente (serio, real y concreto) que nos encontraremos aquí es que muchas de estas plataformas y/o dispositivos son muy caros, y por esa razón no se poseen en maqueta o para pruebas, su criticidad tampoco permite hacer pruebas de restauración, pues ante cualquier fallo de estos dispositivos en producción el impacto es alto, esta es una realidad frecuente, ante la cual también tal vez se pueda hacer recapacitar a quien tenga la decisión de adquirir maquetas, o contratar estas pruebas

por parte de los proveedores de estos dispositivos que sí poseen esas maquetas, y alquilándolos por el tiempo necesario, hacer las pruebas pertinentes de recuperación, obteniendo todas las conclusiones necesarias.

En muchos casos, hemos podido observar que el área de red no tiene ni los medios, ni el conocimiento necesario para realizar el proceso de recuperación, sino que debe solicitárselo al proveedor de esa plataforma y confiar en sus capacidades.

¿Qué aspectos debemos considerar para esta actividad?:

- Que exista un procedimiento de respaldo y recuperación. (Redacción, aprobación y existencia del procedimiento).
- El alcance del procedimiento (áreas a las que aplica y las que no). ¿Es adecuada la implementación de estos procedimientos?, ¿abarca toda la organización?
- Análisis de criticidad de elementos de red.

  Para poder realizar un adecuado plan de recuperación en tiempo y coste eficiente, es imprescindible contar con un análisis de detalle sobre cuáles son los dispositivos o plataformas críticas para la estrategia de negocio. En este control se trata de verificar si esta actividad se realiza y el nivel de detalle alcanzado
- Análisis de criticidad de tiempos de fallo y recuperación.

  Idem anterior, respecto a un análisis de detalle sobre cuáles son los tiempos mínimos y máximos que cada plataforma, área, dispositivo puede soportar.
- Inventario de soportes

  ¿se encuentran debidamente identificados estos soportes?, ¿Existe alguna metodología o procedimiento para este inventariado?
- Plan de pruebas (Desarrollo, hitos fechas y periodicidad, registros de pruebas correctas y erróneas).

  ¿Existe este plan?, ¿se cumple?, ¿hay registros al respecto?
- Planes de mejora (estudios, propuestas, modificaciones al plan y procedimiento, acciones concretas).

  ¿se verifican acciones de mejora generadas por estas pruebas?
- Descripción e implantación de mecanismos de: redundancia, rotación, extracción de discos y cintas, registros de entrada, salida y destrucción de soportes.

  ¿Existen estos mecanismos?, ¿se cumplen?, ¿son adecuados?, ¿hay constancias de ello?
- Nivel de detalle en asignación de roles y responsabilidades.

  Responsables del: elemento, almacenamiento principal y secundario, otros resguardos, plataformas de resguardo y recuperación, acceso a la

información, implantación, actualización y difusión del plan, pruebas de ejecución, etc. Verificación del detalle alcanzado.

Dado que el backup es el último recurso en caso de producirse una situación de pérdida de datos es muy importante definir un procedimiento de backup que sea común a todas las unidades de Red.

Si bien algunos de los aspectos que detallaremos a continuación suelen formar parte del "**Plan de Continuidad de Negocio**", consideramos que es importante hacer hincapié sobre los mismos dentro de un procedimiento de Backups, contemplando al menos los siguientes aspectos clave:

RTO (Restauration Time Objetive): tiempo de restauración del backup o ventana de tiempo en la que el backup ha de ser recuperado. Es decir, ¿en cuánto tiempo debe estar nuevamente en producción? Este punto suele ser motivado por un análisis de riesgo previo, pues no necesariamente deben tener todos los dispositivos la misma prioridad o impacto para la organización a la hora de recuperar su funcionamiento normal.

RPO (Restauration Point Objetive): punto a partir del cual ha de ser posible restaurar el backup expresado en horas, días o semanas según proceda. Es decir, ¿cuántos datos puedo llegar a perder?, ¿Es necesario actualizar cada hora, cada día, cada semana, cada mes? Sobre este punto aplican las consideraciones del punto anterior y a su vez se suma el carácter "dinámico o estático" que tenga cada plataforma o dispositivo, pues existen algunos de ellos cuyas configuraciones no suelen ser modificadas por meses o años (*Ej: grandes Switchs, Proxies*), y por el contrario dispositivos que se modifican varias veces al día (*Ej: LDAP; TACACS, Servidores de Logs*).

Verificación del contenido (Integridad): Comprobación de que el backup contiene todos los objetos necesarios para restaurar el sistema dentro de los objetivos definidos por los dos puntos anteriores. En este punto es muy importante mantener un nivel adecuado de sincronización con el proceso de Gestión de Cambios para garantizar la efectividad de los contenidos del backup.

Pruebas de restauración: Deberá establecerse una plan de pruebas de restauración periódicas para verificar que el contenido y el estado del backup es el adecuado para restaurar el sistema según sus objetivos de RTO y RPO. Para ello se deberá de disponer de un entorno de test para la restauración regular de los backups. De no poseer estos entornos de test o maquetas, se puede contratar con el proveedor de la plataforma, entregando periódicamente a este las copias de seguridad, para que se realicen las verificaciones en sus instalaciones y nos presente un informe de resultados de la actividad.

G**estión de Soportes**: Deberá establecerse una metodología para la clasificación, etiquetado e inventariado de los soportes magnéticos u ópticos, ubicación

de los mismos en un lugar seguro (cámara ignífuga) y off-site para los soportes más críticos, expiración de soportes y políticas de rotación. Dentro de este apartado, es fundamental considerar la destrucción, entrada y salidas de soportes, pues hay pocas cosas más peligrosas para la seguridad que la ausencia de un backup, sin saber cuál fue el paradero del mismo.

3.6. Gestión de Incidencias.

Este procedimiento debe contemplar todas las acciones relacionadas a la notificación, gestión y respuesta a incidentes de seguridad, definiendo claramente las responsabilidades, obligaciones y acciones a realizar en el tratamiento de incidencias.

Uno de los aspectos más importantes en el manejo de incidencias es el de "Recopilación y análisis de evidencias", pues será la información de mayor interés a la hora de evaluar el hecho o realizar un análisis forense.

Existen varias **RFC** (Request For Comments) que regulan o estandarizan metodologías y procedimientos para el manejo de incidencias. Un buen punto de partida es la política de seguridad que propone la **RFC–2196** (Site Security Handbook) y también la anterior **RFC-1244** (que si bien queda obsoleta por la primera es muy ilustrativa), ambas planten una metodología muy eficiente de feedback partiendo desde el plano más alto de la Organización hasta llegar al nivel de detalle, para comparar nuevamente las decisiones tomadas y reingresar las conclusiones al sistema evaluando los resultados y modificando las deficiencias basadas en el control de incidencias.

Sobre el punto en el cual se desea prestar especial atención en esta investigación es, dentro de esta RFC, el **2.5**. (SIC):

" Protect and Proceed

1. *If assets are not well protected.*
2. *If continued penetration could result in great financial risk.*
3. *If the possibility or willingness to prosecute is not present.*
4. *If user base is unknown.*
5. *If users are unsophisticated and their work is vulnerable.*
6. *If the site is vulnerable to lawsuits from users, e.g., if their resources are undermined.*

Pursue and Prosecute

1. *If assets and systems are well protected.*
2. *If good backups are available.*
3. *If the risk to the assets is outweighed by the disruption caused by the present and possibly future penetrations.*

4. *If this is a concentrated attack occurring with great frequency and intensity.*
5. *If the site has a natural attraction to intruders, and consequently regularly attracts intruders.*
6. *If the site is willing to incur the financial (or other) risk to assets by allowing the penetrator continue.*
7. *If intruder access can be controlled.*
8. *If the monitoring tools are sufficiently well-developed to make the pursuit worthwhile.*
9. *If the support staff is sufficiently clever and knowledgable about the operating system, related utilities, and systems to make the pursuit worthwhile.*
10. *If there is willingness on the part of management to prosecute.*
11. *If the system adminitrators know in general what kind of evidence would lead to prosecution.*
12. *If there is established contact with knowledgeable law enforcement.*
13. *If there is a site representative versed in the relevant legal issues.*
14. *If the site is prepared for possible legal action from its own users if their data or systems become compromised during the pursuit."*

En este punto es donde se hace referencia al proceder ante incidentes ya mencionado proponiendo, como acabamos de ver, dos estrategias:

- Proteger y proceder.

- Seguir y perseguir.

La primera de ellas es un curso de acción bajo el cual ante una intrusión, inmediatamente se procede a desconectar sistemas, apagar servidores, negar accesos, etc. Es decir se soluciona el problema actual pero no se puede llegar al fondo del mismo, no permite determinar las causas, ante lo cual cuando se vuelva a su régimen normal, existe una gran posibilidad que la intrusión se produzca nuevamente. Las ventajas que ofrece son que el intruso en ese momento no podrá avanzar más, y la información y recursos serán protegidos. Es una buena metodología a tener en cuenta si no se posee un alto grado de capacitación, soporte especializado ni recursos suficientes.

La segunda metodología es más audaz, permitiendo llegar al origen de la vulnerabilidad, determinar las causas, los pasos que siguió el intruso, obtener toda la información probatoria, e inclusive hasta generar ataques inversos. Lo que es evidente aquí es que se está "Jugando con fuego", es decir se debe tener mucho nivel de conocimientos, herramientas adecuadas, especialistas en apoyo y hasta soporte legal y de difusión de noticias.

Este es el punto clave para el desarrollo de este procedimiento ante incidencias, pues sin un riguroso análisis, diseño e implantación de acciones adecuadas es imposible realizar un "Seguimiento de intrusiones" con un cierto grado de efectividad. por lo tanto se debe plantear una nueva línea de pensamiento para la planificación e implementación de nuestras redes que oriente paso a paso al administrador de las mismos para "convivir" con una incidencia de la mejor forma posible.

En el caso de incidencias que sean generadas por intentos de intrusión, lo realmente crítico que posee este hecho es el absoluto desconocimiento del adversario en cuanto a su ubicación, magnitud, recursos y capacidades. Si a este hecho se suma la necesidad, u obligación actual de exponer información al público en general y a sus socios de negocios, fuente de ingresos de una empresa; y a su vez se tiene en cuenta que esta información día a día va aumentando como una estrategia competitiva de presencia en la red y de rapidez en las negociaciones, esto provoca un mayor grado de exposición y por lo tanto de vulnerabilidades.

¿Qué aspectos debemos controlar especialmente con este procedimiento?:

- Metodología para la notificación, gestión y respuesta a incidentes de seguridad de la información.

  Redacción, aprobación y existencia del procedimiento

- Alcance del procedimiento (áreas a las que aplica y las que no)

  ¿Es adecuada la implementación de estos procedimientos?, ¿abarca toda la organización?. Verificación de hasta dónde se cumple o no lo que establece la documentación.

- Integración con Work flow de la organización.

  En caso todas las organizaciones, existen hoy en día flujos de gestión de actividades, tareas, proyectos, etc. Este procedimiento debería estar integrado a estos flujos de forma tal que facilite la asignación de actividades al personal involucrado y permita realizar un seguimiento detallado de las mismas.

- Nivel de Integración con "Control de cambios".

  Se ha verificado la ocurrencia de muchos incidentes de seguridad que se generan durante acciones de cambio en dispositivos de red, por lo tanto cuando se está realizando este tipo de tareas, debe tenerse en cuenta un "ticket" o flujo que mantenga alerta a la organización para poder dar rápida respuesta si ocurriera este tipo de incidentes, ¿existe este tipo de integración?

- Clara distribución de roles, responsables, funciones y cadena de llamadas.

  ¿Se cuenta con este tipo de documentación?,¿está actualizada?, ¿está al alcance de las personas adecuadas?, ¿funciona correctamente?

- Mecanismos de monitorización, alarmas y escalado de incidencias.

  Una vez ocurrida una incidencia, ¿son correctos estos mecanismos?

- Informes, estadísticas, acciones de mejora.

  ¿Existen evidencias de informes, o estadísticas sobre incidentes de seguridad?, ¿Se verifican acciones de mejora desencadenadas por estos?

- Recopilación de evidencias.

¿es factible recopilar evidencias sobre incidentes de seguridad?, ¿es ágil este mecanismo?, ¿funciona adecuadamente?

3.7. Supervisión y Monitorización.

Para poder ofrecer un grado de "Disponibilidad" mínimo es necesario contar con una infraestructura de "Supervisión y Monitorización". Desde el punto de vista de la Seguridad a su vez, no sólo nos interesa por la disponibilidad, sino también para la detección temprana y la generación de alertas ante cualquier actividad anómala en la misma. Ambas funciones se llevan a cabo a través de:

- **NOC** (Network Operation Center).
- **SOC** (Security Operation Center).

Desde ya que estas funciones deberán ser acordes al tipo de red y se deberá asignar los recursos adecuados para cada tipología, pero lo importante aquí es ser conscientes de la importancia que revista esta actividad y plantearse SIEMPRE cómo se llevará a cabo, por mínima que sea la infraestructura.

En los párrafos siguientes se definirán los aspectos que deben ser tenidos en cuenta, en general se presentan con un "objetivo de máxima", es decir lo ideal que podríamos plantearlos si tuviéramos un NOC y un SOC 24x7, pero reiteramos, lo importante es no olvidarse de esta actividad y ajustarla a la red que cada uno posea.

En cuanto a la Supervisión / Monitorización / Alarmas, nuestra experiencia al respecto es muy positiva. En general todas las redes, poseen algún tipo de mecanismos para esta actividad.

El aspecto sobre el que vamos comenzar es el el "**Flujo y categorización**" de alarmas e incidentes de seguridad. Para ello, inicialmente debemos diferenciar el concepto de "**NOC**: Network Operation Center" del de "**SOC**: Security Operation Center", pues este último sí debería abocarse exclusivamente a seguridad, mientras que el primero no. La cuestión, tal cual planteamos al inicio, está en que no todas las redes poseen SOC (y tampoco se justifica que lo tengan), en estos casos, evidentemente algún tipo de tareas relacionadas a seguridad deberían recaer sobre el NOC.

Sea cual fuere la situación (con o sin SOC), nuestro objetivo en la redacción y aplicación de un procedimiento de este tipo, debería conducirnos a obtener una visión clara sobre:

¿Qué hace este personal si detecta alguna anomalía en la red, cuyos parámetros puedan esta relacionados con un incidente de seguridad?

Ejemplos típicos de ello son:

a) Incremento anómalo de ancho de banda.
b) Saturación del ancho de banda.

c) Caídas secuenciales de dispositivos.
d) Propagación abusiva de un determinado patrón de tráfico.
e) Modificaciones sensibles del flujo de tráfico de nuestros DNSs.
f) Incremento llamativo del volumen de Logs.
g) Mensajes anómalos en los Logs de elementos de red.
h) Alarmas en bases de datos, procesadores, módulos de memoria.
i) Alteración de rutas.
j) Fallos en los sistemas de señalización.
k) Segmentos de red o dispositivos inalcanzables.
l) Pérdidas de accesos de gestión a dispositivos.
m) Modificación de contraseñas, cuentas, perfiles, roles, o directorios activos.
n) Intentos reiterados de accesos (fallidos o no).
o) Escaneos anómalos de red o puertos.
p) Etc.

Con este tipo de ocurrencias, se está ante indicios de algo que puede guardar relación con incidentes de seguridad. En principio para que un procedimiento de gestión de Supervisión / monitorización, podemos indagar acerca de si están o no tipificados estos casos, ¿Existen evidencias de este tipo de anomalías?, en segundo lugar deberíamos analizar si:

a) ¿Existe un procedimiento ante estos casos específicos?
b) ¿Se conocen o definen los pasos a seguir?
c) Dentro del workflow de este centro, ¿está contemplado o tipificado algún “ticket” (o varios tipos de “tickets”) para temas relacionados a seguridad?
d) ¿Está categorizado este flujo para incidentes de seguridad?
e) ¿Se conoce la jerarquía, niveles de escalado o cadena de comunicación para estos casos?
f) ¿Cómo se abre, verifica, mantiene y cierran estas incidencias?

Este tipo de tareas sí son las que hemos verificado que presentan flancos en la mayoría de las redes.

Más consideraciones que deben ser tenidas en cuenta para este procedimiento son:

- Situación de los centros de supervisión de red.

  Que existan en nuestras redes, que posean las herramientas necesarias, que el personal tenga documentadas y comprenda sus funciones, responsabilidades y obligaciones, que los elementos y eventos a monitorizar y supervisar sean acordes al dimensionamiento del centro.

- Que se generen los "Registros de auditoría y monitorización".

  Que se contemple su revisión de forma continua junto a la eficacia y eficiencia de los controles de seguridad establecidos, así como la detección de las anomalías que puedan afectar a la seguridad de la información y los recursos de la empresa.

  Para ello es necesario definir, implantar y/o gestionar:

  - los requisitos y tecnologías de generación y almacenamiento de los registros de auditoría.
  - los procedimientos y tecnologías de monitorización de los registros de auditoría.

  Se deberían registrar todos los eventos de seguridad, es decir, todos los sucesos, ocurrencias o fallos observables en un sistema de información o red de comunicaciones que puedan estar relacionados con la confidencialidad, integridad o disponibilidad de la información. Especialmente se registrarán la actividad de los administradores y operadores de los sistemas de información.

En cuanto a la supervisión:

a. ¿Se registra especialmente la actividad de los administradores y operadores de los sistemas de información?
b. ¿Se realiza algún tipo de análisis para determinar la profundidad o cantidad de eventos a registrar en un sistema de información o red de comunicaciones?
c. En cualquier caso, se supervisan y monitorizan adecuadamente los eventos de seguridad que se detallan a continuación?:
   - los eventos requeridos por la legislación aplicable.
   - los intentos de autenticación fallidos.
   - los accesos de los usuarios a los dispositivos, tanto autorizados como los intentos no autorizados.
   - los eventos de operación y administración de los sistemas: el uso de cuentas privilegiadas de administración (root, admin, etc.), el uso de programas y utilidades de administración, la parada y arranque de los sistemas, la instalación o desinstalación de dispositivos de almacenamiento o de entrada/salida, etc.
   - los cambios en los parámetros de configuración de los sistemas.
   - los errores de funcionamiento de los sistemas y las redes.
   - los accesos a redes de comunicaciones, tanto autorizados como los intentos no autorizados: acceso remoto a la red interna (por Ras, ADSL, red privada virtual, etc.), accesos a Internet, etc.
   - el tráfico no permitido o rechazado por los cortafuegos y los dispositivos de encaminamiento (al menos de los protocolos más comunes y/o peligrosos).
   - las alertas generadas por los dispositivos de detección/prevención de intrusos (IDS/IPS).

- los cambios en los privilegios de acceso: alta, baja y modificación de usuarios, cambios en los perfiles, etc.
- los cambios en los sistemas de seguridad, como la activación/desactivación o cambios en la configuración de los antivirus, de los sistemas de control de acceso, etc.
- el acceso al código fuente de los sistemas desarrollados
- la activación/desactivación o cambios en la configuración de los mecanismos que generan los registros de auditoría
- las modificaciones o borrado de los ficheros con registros de auditoría
- el acceso a datos de carácter personal sensibles

El procedimiento debe establecer claramente que infraestructuras, plataformas, dispositivos, redes y sistemas serán monitorizados y de qué forma se elaborarán y revisarán informes periódicos con los resultados de la monitorización. La periodicidad en la generación y revisión de cada informe estará determinada por el análisis de riesgos del elemento al que aplica.

Se deben considerar también los errores de funcionamiento de los sistemas y redes reportados por los usuarios o generados por las aplicaciones y cómo deberán ser analizados para identificar los posibles problemas de los sistemas.

Se recomienda dentro de lo posible, el uso de un sistema centralizado para la monitorización y supervisión de red que sea independiente del resto de equipos y aplicaciones. Estos sistemas centralizados permiten la definición de reglas de correlación para la identificación de ataques y modelos de comportamiento.

3.8. Gestión de Logs.

El concepto de Logs, muchas veces se relaciona o se denomina como "Registro de Auditoría", lo cual sin entrar en debates sobre si es correcto o no, puede resultarnos interesante pues en definitiva un Log es un tipo de registro que se genera desde un dispositivo para dejar constancia de un evento. Un Log (o registro) para un sistema Unix, que fue el punto de partida de estos temas, es de un tipo u otro dependiendo de la aplicación de la que provenga (facilities) y del nivel de "gravedad" del evento que ha logueado (priorities). El detalle del sistema de Syslog, lo desarrollaremos en el último capítulo. Ahora una vez presentado el tema, nos centraremos únicamente en el procedimiento de "gestión de Logs".

Una de las acciones sobre las que más interés hemos puesto en los últimos años es justamente la implantación de plataformas de centralización de Logs. Hoy en día debemos referirnos a estas como **SIEM**: Security Information and Event Management.

En realidad el concepto de SIEM viene de una combinación de dos soluciones (o definiciones) anteriores:

- **SIM**: Security Information Management
- **SEM**: Security Event Management

Al unir ambas ideas aparece, tal vez más robusta, la posibilidad de "correlar" (o correlacionar) eventos de seguridad. Hoy en día estas implementaciones son de uso frecuente, y existen varios proveedores, algunos de ellos son:

- ArcSight de HP
- RSA Security Analytics
- Splunk (*Puede discutirse si es o no un SIEM…)*

Nuestra experiencia sobre los SIEM y el proceso de Gestión de Logs es que se debe considerar dos aspectos básicos:

1) El nivel de implantación y explotación alcanzado de Logs.

Los indicadores del estado de implantación podemos medirlos en base a:

- Análisis de dispositivos que deben enviar Logs y evaluación de su criticidad.
- Análisis del tipo de Logs a recolectar
- Nivel de implantación en la centralización de Logs.
- Tiempo de puesta en producción de la herramienta.
- Recursos dedicados a la actividad.
- Cantidad de elementos que envían Logs.
- Gestiones a realizar para nuevas integraciones de envíos de Logs.
- Metodología de trabajo de los administradores en el manejo de la herramienta de centralización y/o correlación.
- Tipo de consultas, vistas, informes y estadísticas definidas.
- Informes generados.

Explotación de la plataforma: descubrimientos, elevación, evolución, seguimiento, acciones de mejora que hayan generado estos informes.

- Actualización a la versión más reciente y nivel de parcheado del Servidor de Logs.
- Metodología de resguardo, rotación, compresión y borrado de Logs

2) El nivel de seguridad en la gestión de la plataforma de centralización y/o correlación.

El acceso a la plataforma debe estar realizándose a través de https hacia la interfaz web de acceso.

La validación, debe ser realizada con usuarios que respondan a lo que se establece en el proceso de "Gestión de accesos".

Una actividad importante es contemplar que se esté implantando de forma segura y "ajustada" el acceso de cada dispositivo que envía Logs hacia aquí. Para ello, cada dispositivo cliente de este SIEM, debe encontrarse situado en el segmento correspondiente de acuerdo a lo establecido,

analizando su arquitectura con el plano, la ruta de estos envíos (saltos en routers), y luego en los Firewalls y/o ACLs en router correspondientes deben poseer las reglas verdaderamente "ajustadas" como para que el envío y recepción de Logs sea seguro, pues justamente su intercepción y/o modificación sería un objetivo de alto interés para un intruso. Sobre este punto por ejemplo puntos clave son:

- El que envía Logs (la fuente) es un dispositivo concreto, no un "rango" o segmento de red, por lo tanto la regla debería ser una sólo IP origen. Las excepciones que pueden presentarse sobre este tema, son por ejemplo que exista un segmento claramente identificado y ajustado de red donde se encuentran varias fuentes de Logs (Ej: Core de routers críticos).
- El puerto normal de envío de Logs, es el estándar de "Syslog": UDP 514. Sólo debería encontrarse este como destino.
- Existen excepciones de envíos a este puerto, que por ejemplo se denominan "File Reader" en RSA, por ejemplo cuando el "Colector" (*que es quien debe recolectar los Logs*) necesita obtenerlos de sistemas particulares, caso "Microsoft Exchange", en estos casos necesita hacer empleo del protocolo "**sftp**" a través del puero TCP 22 de forma "bidireccional", por lo tanto pueden ocurrir este tipo de excepciones, siempre y cuando se encuentren debidamente documentadas. Otro tipo de ellas son hacia **ODBC** (Puertos 1433 y 1434), también hacia sistemas propietarios como el caso de los Firewall Check Point con los puertos lea 18184 y 18210, el envío y recepción de **snmp** con puertos UDP 161 y162, en máquinas Windows recientemente se ha habilitado otra alternativa de consultas a eventos por **http** o **https** (TCP 80 y 443). En cualquier caso lo que nos interesa es que en ninguno de ellos existe la necesidad que la regla de filtrado sea "generosa u holgada", SIEMPRE podrá (o deberá) ser puntual ←→ puerto TCP 22, → puerto TCP 1434, → TCP 443, etc..

4. Switching

4.1. Presentación.

Retomando el viejo hábito de analizar la "Seguridad por Niveles", vamos a continuar el texto analizando en este capítulo el nivel 2 del modelo de capas **TCP/IP** (Link level). En el libro anterior ("**Seguridad por Niveles**") ya hemos visto que este nivel de acuerdo a la bibliografía que tomemos como referencia puede ser asociado o no de forma directa con el correspondiente nivel del modelo OSI, durante todo nuestros textos sí lo asociaremos, por lo tanto todo concepto que desarrollemos aquí guardará relación directa con lo que regule **ISO** (International Estándar Organization) en su modelo de capas **OSI** (Open System Interconection).

En este nivel 2 veremos también que un referente que no podemos dejar de lado es **IEEE** (Institute of Electrical and Electronics Engineers) con su subcomité 802.x que es el encargado de estandarizar temas relacionados a redes **LAN** (Local Area Network). En particular, cuando hablamos de redes LAN cableadas, hoy en día el estándar de facto es 802.3 "Ethernet" (o CSMA/CD: Carrier Sence Multiple Access / Collition Detect), por lo tanto nos centraremos en esta norma, y para el caso de las redes WiFi, lo haremos respetando lo que establece 802.11. También veremos otros aspectos de la familia 802.x que especifican aspectos de autenticación, control de accesos, etc.

¿Por qué llamamos "**Switching**" a este capítulo?

Porque queremos marcar bien la diferencia entre el conjunto de actividades que debemos realizar en el nivel de **enlace** y las del nivel de **red**. Este importante detalle desde el punto de vista de la seguridad implica un cúmulo de aspectos que cuando son bien comprendidos facilitan y estructuran mucho más la seguridad de nuestras redes pues son tareas que no deben ser mezcladas. A pesar de que, como reiteramos muchas veces, los dispositivos actuales con su potencia suelen asumir tareas de más de un nivel, para nosotros SIEMPRE será diferente una función de nivel 2 que llamaremos en su conjunto "Switching" de una de nivel 3 que llamaremos en su conjunto "Routing".

El dispositivo por excelencia en grandes redes LAN que opera en este nivel es el "Switch". La familia dominante en las grandes redes son el Cisco Catalyst y el Cisco Nexus. De toda esta gama de Cisco, los más frecuentes son los de la línea 6500.



Imagen 4.1 (Familia de Switchs Cisco 65xx)

El término Switch podemos interpretarlo como "Conmutación" (de hecho en electricidad es así). Desde el punto de vista de redes, este término nace cuando se empiezan a dividir los "Dominios de colisión" de las redes Ethernet, dejando de lado los viejos "**Hubs**" para poder optimizar el rendimiento de esta estrategia de tráfico basada en el control del canal de comunicaciones mediante la "Escucha y el acceso por colisión". Todo el detalle sobre este funcionamiento podemos verlo en el Capítulo 4 del libro "**Seguridad por Niveles**" así que no redundaremos en estos conceptos. Lo que sí es importante recalcar es que este nivel opera basado en el encabezado de nivel 2 regulado como "**Ethernet**" u "**802.3**" (que recordemos que si bien no son iguales, su operativa es "casi" la misma), dentro de sus catorce bytes están los 6 byte de dirección origen, los 6 byte de dirección destino y los 2 byte del campo "Ethertype" o "Lenght", sin considerar los 4 byte de CRC (Control de Redundancia Cíclica), lo 7 byte de preámbulo y el byte de arranque.

El formato de una trama Ethernet es el que se detalla a continuación:

8	7	6	5	4	3	2	1
Dirección destino (6 Byte)							
Dirección Origen (6Byte)							
Tipo o longitud (2 Byte)							
Datos (Variable entre 46 y 1500 Byte)							
CRC (4 Byte)							

- Dirección destino: Especifica la dirección del host a alcanzar a nivel MAC.
- Dirección origen: Especifica la propia dirección a nivel MAC.
- Tipo o longitud: Si se trata del protocolo Ethernet el tipo de protocolo de nivel superior (Ethertype). Si es protocolo 802.3 especifica la longitud del campo de datos
- CRC: Control de redundancia cíclica, emplea el concepto de polinomio generador como divisor de la totalidad de la trama, el resto de esta operación se enmascara con una secuencia d-determinada de bit y se envía en este campo. Se trata entonces de una división binaria, en la cual se emplea como polinomio generador justamente el CRC-32, que figura abajo, por lo tanto el resto de esta división SIEMPRE será una secuencia de bit de longitud inferior a 32 bits, que será lo que se incluye en este campo. Los formatos estandarizados de estos CRCs son los que se presentan a continuación:

  •**CRC-12**: $X^{12} + X^{11} + X^3 + X^2 + X + 1$

  •**CRC-16**: $X^{16} + X^{15} + X^2 + 1$

  •**CRC CCITT V41**: $X^{16} + X^{12} + X^5 + 1$ (este código se utiliza en el procedimiento *HDLC*)

  •**CRC-32** (**Ethernet**): $= X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

  •**CRC ARPA**: $X^{24} + X^{23} + X^{17} + X^{16} + X^{15} + X^{13} + X^{11} + X^{10} + X^9 + X^8 + X^5 + X^3 + 1$

- Preámbulo: No está representado en la gráfica anterior, pues no es considerado como parte de la trama pero se trata de 7 byte que indican que comienza una trama y permite sincronizar relojes, y 1 octavo Byte de inicio.

Desde el punto de vista de la Seguridad en Redes, nos interesa comprender qué podemos hacer con este encabezado y qué tipo de herramientas podemos emplear para que este nivel opera de acuerdo a lo deseado. Respetando lo que define IEEE en su subcomité 802, sigamos tratando la seguridad en este nivel 2 paso a paso.

4.2. Familia 802.1

El Grupo **802.1** Podemos resumirlo en algunas tareas fundamentales:

- Arquitectura e interconexión LAN/MAN.
- Seguridad.

- Gestión global de la red.

¿Qué nos interesa de ellas desde el punto de vista de seguridad en este texto?:

- **802.1D**: Spanning Tree Protocol
- **802.1aq:** Shortest Path Bridging (SPB)
- **802.1Q**: Virtual Local Area Networks (VLAN)
- **802.1x**: Autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible RFC 3748 (EAP).
- **IEEE 802.11** – Redes inalámbricas WLAN.

4.2.1. 802.1D (Spanning Tree Protocol: **STP**).

Uno de los peores problemas que puede presentarse para un Switch es cuando escucha la misma dirección **MAC** (Medium Access Control) por dos interfaces físicas diferentes, este es un bucle que en principio, no sabría como resolver. Este problema si bien parece poco probable que pueda ocurrir, en realidad en redes grandes al tener cientos o miles de cables (muchos de ellos para redundancia), este hecho es tan sencillo como conectar el mismo cable en diferentes patch pannels que cierran un lazo sobre el mismo dispositivo, y en la realidad ocurre con cierta frecuencia, mayor, en la medida que más grande sea la red LAN. También es un hecho concreto cuando el cableado se diseña para poseer caminos redundantes, justamente para incrementar la disponibilidad de la red.

Cuando físicamente se cierra un bucle, la topología pura de red "Jerárquica" deja de serlo y se convierte en una red "Malla". Para tratar este problema el protocolo Spanning Tree crea una red "Jerárquica lógica (árbol Lógico)" sobre esta red "Malla Física". Este protocolo crea "Puentes" (bridges) de unión sobre estos enlaces y define a través de diferentes algoritmos que se pueden configurar, cuál es el que tiene mayor prioridad, este puente de máxima prioridad lo denomina "Root Bridge" (o Puente Raíz) y será el que manda jerárquicamente las interfaces por las cuáles se separarán los diferentes dominios de colisión. Todo el control de STP se realiza mediante tramas llamadas **BPDU** (Bridge Protocol Data Unit) que son las que regulan los diferentes dominios de colisión . El parámetro que define esta jerarquía es el **BID** (Bridge Identifier) que está compuesto por el Bridge Priority + dirección MAC. El Bridge Priority es un valor configurable que por defecto está asignado en 32768.

En general este protocolo se configura de forma automática, y se basa en el orden de encendido de los diferentes Switchs de la red, siendo el primero que se

pone en funcionamiento el que se auto designa "Root Bridge", pero por supuesto se puede realizar de forma manual.

Cada switch reemplaza los BID de raíz más alta por BID de raíz más baja en las BPDU. Todos los switches que reciben las BPDU determinan en sus tablas que el switch que cuyo valor de BID es el más bajo será "su" puente raíz, y a su vez envían nuevas BPDU hacia sus otras interfaces con un ID más alto, incrementando el parámetro "Root Path Cost" *(Que veremos en el ejemplo que sigue)* informando con esta nueva BPDU a todo dispositivo que esté conectado físicamente a él cómo debe ir armándose este árbol . Si se desea configurar de forma manual, el administrador de red puede establecer jerarquía que desee configurando la prioridad de switch que sea "Root Bridge" en un valor más pequeño que el del valor por defecto (32768, todo valor debe ser múltiplo de 4096), lo que hace que este BID sea más pequeño y a partir de este "root" puede configurar la jerarquía o árbol si lo desea, o también al reconocer los demás switch a este "root", de forma automática pueden generar el resto del árbol.

System ID Extension. (dentro de una trama BPDU).

El ID de puente es un campo dentro de un paquete BPDU que tiene ocho bytes de longitud. Los dos primeros bytes son la prioridad de puente, un entero sin signo de 0-65.535. Los últimos seis bytes, son la dirección MAC suministrada por el puente. Desde IEEE 802.1D-2004, de los dos primeros bytes, los cuatro primeros bits son una prioridad configurable, y los últimos doce bits llevan la extensión ID del dispositivo que generó esta trama (puente en la nomenclatura STP).

Un tema que debemos mencionar, pues va de la mano del concepto de VLAN que veremos más adelante, es el protocolo Spanning Tree múltiple o **MSTP** (Multiple Spanning Tree Protocol). En el mismo, la extensión ID del sistema puente lleva el número de instancia MSTP. Esta definición tiene lugar pues algunos vendedores propusieron emplear la extensión ID sistema para llevar un ID de VLAN permitiendo un árbol de expansión por cada VLAN que se haya definido en la red.

MSTP es una evolución del protocolo Spanning Tree. Fue introducido en **802.1s** IEEE como una enmienda a 802.1Q (*VLAN, que veremos más adelante*) en su edición de 1998, más tarde fusionado con IEEE **802.1Q-2005**. Se define esta extensión para poder desarrollar aún más la utilidad de las redes de área local virtuales (VLAN). Si sólo hay una LAN Virtual (VLAN) en la red no se emplea. Si la red contiene más de una VLAN, la red lógica configurada por una sola STP funcionaría perfectamente, pero es posible hacer un mejor uso de la red (y asegurar su "**visibilidad**" y "**Segmentación**") mediante el uso de un árbol de expansión alternativo para cada VLAN o grupos de VLAN.

A continuación presentamos dentro de una captura de trama Ethernet, solo el protocolo STP (Hemos resaltado en negrita los campos que estamos desarrollando en este texto) :

Spanning Tree Protocol
Protocol Identifier: **Spanning Tree Protocol** (0x0000)
Protocol Version Identifier: Spanning Tree (0)
BPDU Type: Configuration (0x00)
BPDU flags: 0x00
0... .... = Topology Change Acknowledgment: No
....0 = Topology Change: No
Root Identifier: 4096 / 253 / 00:22:0d:e8:38:00
Root Bridge Priority: 4096
Root Bridge System ID Extension: 253
Root Bridge System ID: 00:22:0d:e8:38:00
Root Path Cost: 0
Bridge Identifier: 4096 / 253 / 00:22:0d:e8:38:00
Bridge Priority: 4096
Bridge System ID Extension: 253
Bridge System ID: 00:22:0d:e8:38:00
Port identifier: 0x941d
Message Age: 0
Max Age: 20
Hello Time: 2
Forward Delay: 15
Originating VLAN (PVID): 253
Type: Originating VLAN (0x0000)
Length: 2
Originating VLAN: 253

En la captura anterior vemos en particular, el envío de esta BPDU desde un root (4096) que forma parte de la VLAN 253 y su dirección MAC es: 00:22:0d:e8:38:00.

Analicemos cada campo en detalle:

- PID (2 bytes): Protocolo, siempre cero
  Protocol Identifier: **Spanning Tree Protocol** (0x0000)
- Version (1 byte): Versión de STP, puede ser cero (STP), uno (RSTP) o tres (MSTP)
  Protocol Version Identifier: Spanning Tree (0)
- Message type (1 byte): Tipo de BPDU: configuration (0x00) o TCN (0x80
  BPDU Type: Configuration (0x00)
- Flags (1 byte): diversos parámetros (útil para RSTP) y un bit para notificar un cambio de topología

  BPDU flags: 0x00
  0... .... = Topology Change Acknowledgment: No
  ....0 = Topology Change: No
- Root ID (8 bytes): ID del dispositivo raíz

  Root Identifier: 4096 / 253 / 00:22:0d:e8:38:00
  Root Bridge Priority: 4096
  Root Bridge System ID Extension: 253
  Root Bridge System ID: 00:22:0d:e8:38:00

- Root path cost (4 bytes): coste del camino hasta el dispositivo raíz
  Root Path Cost: 0
- Bridge ID (8 bytes): ID del dispositivo que envía la BPDU

  Bridge Identifier: 4096 / 253 / 00:22:0d:e8:38:00
      Bridge Priority: 4096
      Bridge System ID Extension: 253
      Bridge System ID: 00:22:0d:e8:38:00
- Port ID (2 bytes): número de puerto (IEEE or Cisco STP BPDU) desde el cual se ha enviado la BPDU
  Port identifier: 0x941d
- Message age (2 bytes): tiempo transcurrido desde que el dispositivo raíz envió el mensaje de configuración en el cual se basa el actual
  Max Age: 20
- Maximum age (2 bytes): cuándo debería borrarse el actual mensaje de configuración
  Hello Time: 2
- Hello time (2 bytes): tiempo que transcurre entre el envío de dos BDPU Configuration
  Hello Time: 2
- Forward delay (2 bytes): tiempo que los bridges deberían esperar antes de efectuar la transición a un nuevo estado tras un cambio de topología.
  Forward Delay: 15

Como estamos viendo, el protocolo STP controla toda la configuración de este árbol lógico por medio de estas tramas BPDU, las cuáles en realidad son de dos tipos:

- Configuración: Se envían periódicamente (por defecto son cada 2 segundos).
- TCN (Topology Change Notification): Sólo se envían cuando existe un cambio en la red.

Para ver en la práctica cómo funciona este protocolo, trabajaremos con ejemplos sobre switchs Cisco que suele se el más conocido fabricante de nivel 2 y 3. En los switchs Cisco podemos consultar el árbol con el comando:

```
Switch_ACE# show spanning-tree
      VLAN253
       Spanning tree enabled protocol mstp
       Root ID    Priority    32770
             Address     0010.d321.2301
             Cost       20000
             Port       100 (GigabitEthernet1/4)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

       Bridge ID  Priority    32770  (priority 32768 sys-id-ext 2)
             Address     0010.d321.2402
```

```
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface       Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- -----------------------
Gi1/4           Root FWD 20000     128.135  P2p
Po1             Desg FWD 20000     128.822  P2p
```

Si alguien deseara generar problemas en esta LAN podría, por ejemplo generar tramas BPDU intentando modificar las prioridades que acabamos de ver en la captura de la trama BPDU, o también generar ataques "**ARP Spoofing**" (*como vimos en el ejemplo de ataques a* ***SIP***) para que el switch comience a escuchar direcciones MAC duplicadas por diferentes interfaces, la reacción del mismo será ir deshabilitando esas nuevas interfaces. Esta situación de deshabilitar y habilitar interfaces, se conoce en la jerga de redes como "Flapeo". En situaciones normales, suceden "flapeos" cuando circulan tramas erróneas, se apaga algún dispositivo, se cambia una tarjeta de red, se satura algún vínculo, etc. Si la situación comienza a ser abusiva, el rendimiento de los switchs comienza a degradarse hasta llegar el caso de caerse toda la red (situación que en la realidad sucede más de lo deseado…).

Existen muchas herramientas para generar tramas BPDU fraudulentas, tal vez la más difundida sea "**yersinia**", por mi parte mantengo aún la vieja escuela de "**némesis**". Para ataques ARP spoofing, vimos también al tratar el protocolo SIP el empleo de "**Cain**", pero para ambos casos hay muchas más. Cualquiera de ellas está en capacidad de comprometer el protocolo STP si no se toman medidas básicas.

La primer medida básica de seguridad a adoptar para STP es activar algún mecanismo que reaccione ante saturaciones de BPDU, en el caso de Cisco se trata del comando "bpduguard":

```
Switch_ACE# config term
Switch_ACE(config)# errdisable recovery cause bpduguard
Switch_ACE(config)# errdisable recovery interval 20
Switch_ACE(config)# interface  GigabitEthernet 1/4
Switch_ACE(config-if)# spanning-tree bpduguard enable
```

Con este comando, cuando la interfaz configurada comienza a recibir un volumen anormal de tramas BPDU, deshabilita el puerto (en este ejemplo el GigabitEthernet1/4) esta situación, también puede ser peligrosa, pues si se generan esta tramas sobre las diferentes interfaces del switch, entonces irá deshabilitando cada una de ellas dejando, el propio switch, toda la red fuera de servicio. Para ello, como hemos visto en las primeras líneas del ejemplo (*errdisable recovery cause bpduguard* y *errdisable recovery interval 20*) existe un parámetro de recuperación en el tiempo que decidamos configurar (en nuestro ejemplo 20 segundos).

Existen muchas opciones más de recuperación para un switch, aquí abajo presentamos algunas de ellas:

errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause gbic-invalid
errdisable recovery cause l2ptguard
errdisable recovery cause psecure-violation
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause unicast-flood
errdisable recovery cause arp-inspection
errdisable recovery interval 30

Cuando nuestra jerarquía lógica (Root Bridge) sea conocida, es decir que el administrador haya definido cuál es el "root" de la red, en Cisco existe otro comando más eficiente aún "**guard root**" el cual sólo deshabilita el puerto, si recibe BPDU con Bridge ID de menor valor:

Switch_ACE(config)# interface GigabitEthernet 1/4
Switch_ACE(config-if)# ***spanning-tree guard root***

Por último y nuevamente, siempre que conozcamos la estructura de nuestro "Arbol lógico", podemos filtrar todo el tráfico BPDU sobre las interfaces que no forman parte de la jerarquía, en este caso, nuevamente tomando como ejemplo un switch Cisco, el comando sería:

Switch_ACE(config)# interface GigabitEthernet 1/4
Switch_ACE(config-if)# ***spanning-tree bpdufilter enable***

Existen comandos para hacerlo sobre todos los puertos y más opciones también, pero lo que deseábamos en estas líneas, sin extendernos excesivamente, es poder comenzar a transmitir cómo se comienzan a adoptar medidas sobre cada protocolo y cada nivel para asegurar nuestras redes.

Los principales problemas de STP son la poca flexibilidad para habilitar caminos alternativos y la falta de autenticación de los diferentes dispositivos que envían y reciben BPDU.

Para dar solución a estos problemas, el protocolo STP ha ido evolucionando (**802.1w**, **802.1s**), pero en este texto nos centraremos directamente en **802.1aq** por ser el que hoy en día más nos ofrece.

4.2.2. 802.aq Shortest Path Bridging (**SPB**).

Este protocolo aparece en al año 2006, si bien es alrededor del año 2012 cuando se difunde todo su desarrollo completo. La principal característca que ofrece SPB es que permite mantener "activos" todos los enlaces redundantes, sin necesidad de deshabilitar los bucles físicos (*como hace STP*), manteniendo una real topología de "Malla", con ello mejora la eficiencia y los tiempos de convergencia de la red.

La base de SPB es el protocolo de control denominado **IS-IS** (Intermediate System to Intermediate System), regulado por la **RFC-6329** "IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging" de la cual haremos un resumen a continuación.

SPB puede operar de formas:

- Shortest Path Bridging - **VID (SPBV)** Virtual ID: múltiples VLAN se pueden usar para distribuir la carga en diferentes árboles del camino más corto.
- Shortest Path Bridging - **MAC (SPBM)** Sus decisiones están basadas en el concepto de "**I-SID**" (*Ethernet Services Instance, se emplea para agrupar "E-LAN" que son enlaces lógicos entre dos interfaces físicas Ethernet*), aunque también las VLAN se pueden utilizar para distribuir la carga en diferentes árboles del camino más corto.

En la teoría la gran diferencia para el empleo de uno u otro es que SPBV se pensó para redes de hasta 100 nodos y SPBM hasta 1.000

Hoy en día a nivel 2 hay que sumar un nuevo problema muy frecuente en grandes redes y es la necesidad de separar lógicamente varias zonas de la mismo switch (o conjunto de switches), lo que se suele llamar Multitenancy (Multiple tenencia) y el caso más frecuente, es la necesidad de dar servicio a varios clientes completamente independientes y cuyos flujos de información deben estar debidamente securizados el uno respecto al otro.

Sobre este tema es que surge otra diferencia entre ambos: SPBV utiliza el encapsulamiento **Q-in-Q** (regulado por **802.1ad**), mientras que SPBM utiliza **MAC-in-MAC** (regulado por **802.1ah**). En grandes líneas:

Q-in-Q no es más que utilizar dos etiquetas para las VLANs, una para el segmento del cliente y otra para el del proveedor. Cuando el tráfico de las VLANs de un cliente entra en la red del proveedor, el mismo se re-encapsula dentro de una nueva VLAN, y así circula por la LAN del proveedor "encapsulando" las VLAN de cada cliente. Esta técnica proporciona 16 millones de posibles "VLANs" (4096 del cliente x 4096 del proveedor).

La técnica de MAC-in-MAC, es similar a la anterior, pero encapsula las tramas del cliente dentro de una nueva trama Ethernet con una MAC del propio proveedor, por lo tanto dentro de la red del proveedor, un cliente enviará y recibirá tráfico identificado por otra MAC diferente. Esta técnica separa

completamente los dominios de colisión del cliente y del proveedor, esto optimiza también el tráfico por una cuestión de tablas de aprendizaje diferentes entre cliente y proveedor, por esta razón es que su diseño fue pensado para más dispositivos.

Cabe mencionar que ya existen técnicas más eficientes aún por parte de los diferentes fabricantes (*TRILL, MLAG, Qfabric, FabricPath, etc.)* y también metodologías de encapsulamiento, pero en la actualidad aún no se encuentran estandarizadas al 100% por lo que no las desarrollaremos en este texto. Es cierto que a la hora de tomar alguna decisión sobre escalar STP es muy probable que hoy por hoy debamos caer en alguna de estas soluciones propietarias pues parece ser que aún no existe un acuerdo unánime por su parte para encarar protocolos estandarizados.

Para una verdadera escalabilidad, veremos más adelante que la técnica que más aplica es la de **MPLS** (Multi Protocol Label Switching).

4.2.3. 802.1Q (Virtual LAN).

Este protocolo es el empleado justamente para la creación de VLANs dentro de un mismo switch y poder separar diferentes "dominios de colisión" bajo el concepto de "**Trunking**", lo veremos con mucha frecuencia y desde el punto de vista de la seguridad merece la pena prestarle atención pues es un foco importante de problemas.

802.1Q como veremos a continuación, permite la creación de VLANs, agregando un encabezado de 4 bytes dentro de la misma trama Ethernet. Para que un Switch "**encapsule 802.1q**" debe tener configurada sus interfaces y sus VLAN para ello. Las buenas prácticas, nos indican que si tenemos más de un switch, es mejor hacerlo bajo la idea de Interfaces "**Trunk**" (o troncal), que no son otra cosa que enlaces físicos entre los dispositivos (generalmente Switchs, aunque no exclusivo de estos) por los cuales "entroncaremos" (*aunque suene feo…)* varias VLAN, transportando el tráfico de varias de estas a la vez creando una especie de jerarquíe entre ellos. Existe una VLAN por defecto que es la **VLAN 1** (o VLAN nativa), la cual ante cualquier error, omisión o ausencia de configuración, será por la que el switch envía toda trama y sin agregar ningún encabezado 802.1Q, por esta razón es que esta VLAN 1 SIEMRE debe estar deshabilitada como medida de seguridad, debiendo tener precaución (en cuanto a switching) de cómo opero o creo esta ruta por defecto o nativa en mi switch. Por supuesto que cada VLAN que es configurada en un extremo de cada Trunk debe ser idéntico en el otro pues en definitiva se trata de una conexión punto a punto, para operar en modo Trunk una interfaz debe ser puesta en "tkunk On" (*Switch_ACE(config-if)#switchport mode trunk*) sino por defecto no es trunk. A continuación presentamos cómo se verían estas líneas en un switch (primero se crean las VLAN y luego se asignan):

```
vlan 2
 name Empresa-A
```

```
!
vlan 3
 name Empresa-B
!
vlan 4
 name Empresa-C
!
vlan 10
 name Zona_X
!
vlan 20
 name Zona_Empleados
!
vlan 100
 name Telefonia_IP
........
....
.

interface Port-channel1
 description conexion con Zona_X
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,10,18,35,92-105
 switchport mode trunk
!
interface Port-channel2
 description conexion con Zona_Empleados
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,10,67,94,95
 switchport mode trunk
!
interface Port-channel3
 description conexion con Empresa_A
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,10,21,61-67,70
 switchport mode trunk
......
...
.
```

Para distinguir el tráfico de las diferentes VLANs, a las tramas ethernet se le añade un campo de 4 octetos (trama ethernet extendida), que contiene:

- Tag Protocol Identifier: 16 bits, contiene el valor **0x8100** , para que se identifique la trama como una trama etiquetada.
- Priority: 3 bits, indica la prioridad de la trama, 0 es el más bajo (best effort), 7 el mayor.
- CFI (Canonical Format Indicator): 1 bit, siempre 0 para switches Ethernet.
- VLAN ID: 12 bits que especifican la VLAN a la que pertenece la trama, es posible tener 4096 VLANs.

A todo el tráfico que entra por un puerto de acceso configurado para el empleo de 802.1q (o dot q) el switch añade el campo relativo a la VLAN. Cuando la trama viaja por el trunk, queda intacta, y cuando sale por el puerto destino, el switch quita el campo.

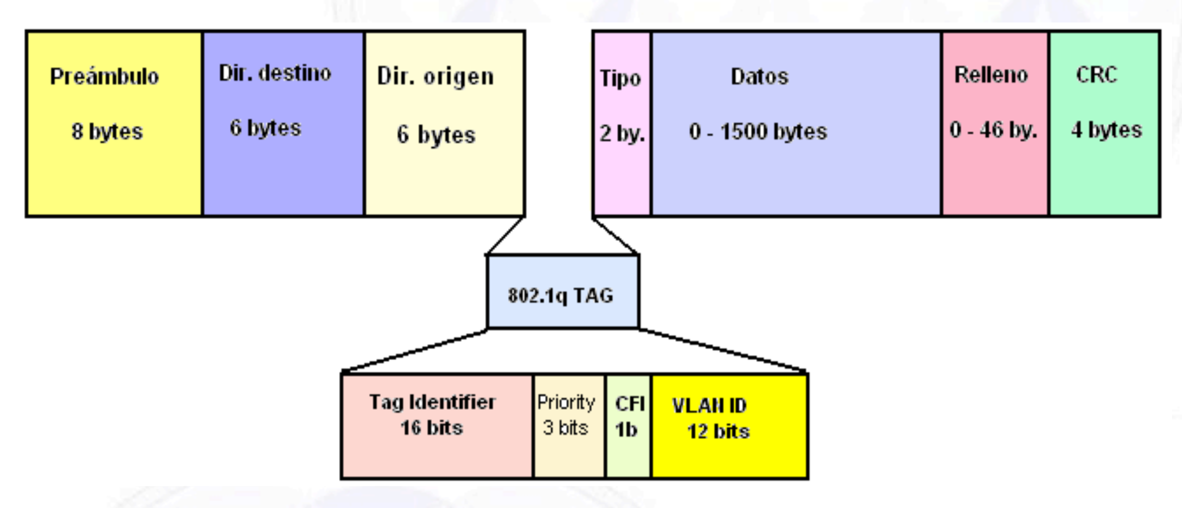


Imagen 4.2 (Formato de una trama 802.1q)

En la imagen anterior, se presenta este formato especial de trama de nivel 2, pues lo que deseamos resaltar es que en la parte superior lo que vemos es una trama Ethernet pura y completa. Antes del campo "Ethertype" de la misma (de dos octetos), vemos que aparece un nuevo "Tag" es lo que hemos presentado en los primeros párrafos como Tag Protocol Identifier de 16 bits, el cual cuando contiene el valor **8100**, a partir de allí cualquier dispositivo de nivel 2 sabe que en este caso particular deberá procesar cuatro octetos "adicionales" que son los que sí sin lugar a dudas identifican al protocolo 802.1Q con su VLAN correspondiente. Esta es la metodología empleada en casi todas las grandes redes para la gestión de VLANs.

Veamos una captura de tráfico 802.1Q:

```
Ethernet II, Src: 60:67:20:8b:13:b4, Dst: 33:33:00:01:00:02
  Destination: 33:33:00:01:00:02
  Source: 60:67:20:8b:13:b4
  Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 13
  000. .... .... .... = Priority: Best Effort (default) (0)
  ...0 .... .... .... = CFI: Canonical (0)
  .... 0000 0000 1101 = ID: 13
```

Type: IPv6 (0x86dd)

Estamos viendo en la práctica los campos de la imagen anterior:

- Un encabezado Ethernet con su:
  - Dirección Destino.

    Destination: 33:33:00:01:00:02
  - Dirección Origen.

    Source: 60:67:20:8b:13:b4
  - Campo Ethertype (*Al final de toda la captura*).

    Type: IPv6 (0x86dd)
- Un encabezado 802.1Q con su:
  - Type.

    Type: 802.1Q Virtual LAN (0x**8100**)
  - Priority.

    000. .... = Priority: Best Effort (default) (0)
  - CFI.

    ...0 .... = CFI: Canonical (0)
  - ID.

    .... 0000 0000 1101 = ID: 13

Antes de seguir adelante con el desarrollo de VLAN, detengámonos un poco a analizar el concepto de "Virtualización" centrado en redes.

El concepto de "redes virtuales" es un término genérico que se emplea para diferentes tecnologías de virtualización, en el caso de redes nos interesa particularmente centrarnos en el empleo del nivel de hardware y la conectividad física para a través del mismo poder "escalar" a los niveles de enlace y red en relaciones de "n" a "n", es decir poder relacionar un nivel físico a varios de enlace o red, o viceversa: varios niveles físicos hacia uno de enlace, varios o uno de red, etc.

El concepto que sí debemos tener claro es que:

- a nivel físico (nivel 1): Las técnicas de "multiplexación" permiten que una misma interfaz física se pueda ver como varios "canales" diferentes y separados entre sí.
- a nivel de enlace (nivel 2): Protocolos como ATM o Frame Relay ofrecen circuitos y rutas virtuales en este nivel (VCI y VPI), y en Ethernet metodologías de VPN a nivel de enlace.
- a nivel de red (nivel 3): Toda la lógica de rutas a nivel IP, permite el empleo de múltiples sesiones a través de una sola interfaz, por medio de la cual pasa un sinnúmero de tráfico de diferente tipo.

Basado en los conceptos anteriores, es que cuando se habla de "redes virtuales" hay que tener claro de qué nivel o niveles se está hablando y cuál es la intención de las mismas pues, dependiendo de la elección, pueden verse o no entre sí, capturar o no su tráfico, cifrar, autenticar, etc. Y eso sí es lo que nos interesa desde el punto de vista de seguridad.

Solo vamos a presentar brevemente el nivel de red para comprender mejor cómo se pueden relacionar entre sí las diferentes metodologías de virtualización y a su vez, para que nos sirva como introducción con MPLS que es el próximo tema a tratar.

En el caso que presentaremos, los routers poseen una tabla global de rutas que contiene la totalidad de sus interfaces, y luego si existen rutas virtuales (de nivel 3) poseerá tablas virtuales para cada "red virtual" que se haya definido asignadas cada una de ellas a interfaces físicas. El concepto de Virtual Route Forward (**VRF**) es una técnica por medio de la cual se crean múltiples redes virtuales con una simple "entidad de red".

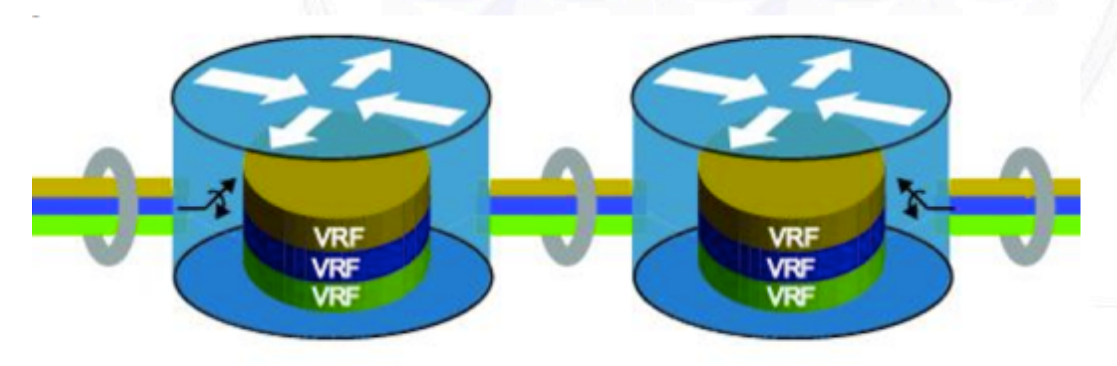


Imagen 4.3 (Esquema de vrf)

La imagen anterior, nos ofrece la visión de cómo los router separan cada paquete que les llega en diferentes VRFs y los enrutará por la interfaz que tenga configurada cada una de ellas (de forma estática o dinámica, que trataremos un poco más abajo). Aquí radica una gran diferencia respecto al concepto de VLAN de nivel dos (enlace)........ ¡¡¡Ojo con esta idea que es fundamental!!!. Cada paquete circulará exclusivamente por esa ruta que está configurada (no por otra) y saldrá exclusivamente por la interfaz física que tenga configurada esa VRF.

Cuando analizamos esto mismo a nivel 2 (enlace), la cosa no es así, pues las tramas de cada VLAN nivel 2 están saliendo por la misma interfaz física, sólo las diferencia el "**encabezado" 802.1q**, pero si cualquiera "escucha" este flujo, verá pasar absolutamente todas las ramas.

En el siguiente caso práctico se puede observar con total claridad:

```
No.     Time              Source                Destination           Protocol Length Info
Frame 1: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
Ethernet II, Src: 60:67:20:8b:13:b4 (60:67:20:8b:13:b4), Dst: 33:33:00:01:00:02
(33:33:00:01:00:02)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 13
```

```
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 0000 1101 = ID: 13
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::b8b6:af45:1136:5186 (fe80::b8b6:af45:1136:5186), Dst:
ff02::1:2 (ff02::1:2)
User Datagram Protocol, Src Port: 546 (546), Dst Port: 547 (547)
DHCPv6

No.     Time            Source                Destination           Protocol Length Info
Frame 2: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
Ethernet II, Src: b4:99:ba:e0:b9:22 (b4:99:ba:e0:b9:22), Dst: 33:33:00:01:00:02
(33:33:00:01:00:02)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 153
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 1001 1001 = ID: 153
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::f1f8:446c:2621:d68f (fe80::f1f8:446c:2621:d68f), Dst:
ff02::1:2 (ff02::1:2)
User Datagram Protocol, Src Port: 546 (546), Dst Port: 547 (547)
DHCPv6

No.     Time            Source                Destination           Protocol Length Info
Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: 00:00:0c:07:ac:05 (00:00:0c:07:ac:05), Dst: 01:00:5e:00:00:02
(01:00:5e:00:00:02)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 5
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 0000 0101 = ID: 5
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.2.5.252 (10.2.5.252), Dst: 224.0.0.2 (224.0.0.2)
User Datagram Protocol, Src Port: 1985 (1985), Dst Port: 1985 (1985)
Cisco Hot Standby Router Protocol

No.     Time            Source                Destination           Protocol Length Info
Frame 6: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: 60:67:20:85:b6:e8 (60:67:20:85:b6:e8), Dst: 33:33:ff:ee:ca:71
(33:33:ff:ee:ca:71)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 213
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 1101 1111 = ID: 213
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::a21c:2ec2:90ee:b16e (fe80::a21c:2ec2:90ee:b16e), Dst:
ff02::1:ffee:ca71 (ff02::1:ffee:ca71)
Internet Control Message Protocol v6

No.     Time            Source                Destination           Protocol Length Info
Frame 13: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: 00:00:0c:07:ac:13 (00:00:0c:07:ac:13), Dst: 01:00:5e:00:00:02
(01:00:5e:00:00:02)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 19
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 0001 0011 = ID: 19
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.112.28.254 (10.112.28.254), Dst: 224.0.0.2 (224.0.0.2)
User Datagram Protocol, Src Port: 1985 (1985), Dst Port: 1985 (1985)
Cisco Hot Standby Router Protocol
```

```
No.     Time             Source                 Destination           Protocol Length Info
Frame 28: 522 bytes on wire (4176 bits), 522 bytes captured (4176 bits)
Ethernet II, Src: 00:20:60:28:0c:45 (00:20:60:28:0c:45), Dst: 01:80:c2:00:00:14
(01:80:c2:00:00:14)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 200
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 1100 1000 = ID: 200
    Length: 504
Logical-Link Control
ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol
* HTTP/1.1
```

En las capturas de tráfico presentadas, se puede apreciar que todas las VLANs (ID: 5, 213, 19, 200) están viajando por el mismo segmento de red (*es en ese mismo donde se ha realizado la captura*), luego la tarjeta de red de cada dispositivo, cuando analice el encabezado 802.1Q decidirá si lo entrega al nivel superior o lo descarta (si no va dirigida a ese dispositivo), pero lo que nos debe quedar claro es que la totalidad de la información es "visible" si escuchamos en este segmento de red.

La configuración de las VLANs nacen en el nivel 2 (enlace) cuyo dispositivo por excelencia es el "Switch". En el mismo se deben "agrupar" qué VLANs se adjudican a cada una de sus bocas físicas, abajo presentamos un ejemplo de ello:

```
Ejemplo-SW_ACE#sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    BACKBONE                         active
5    SALIDA-FIREWALL                  active
6    VLAN0001                         active
7    VLAN0002                         active
8    BACKBONE-REDUNDANTE              active
12   MZ                               active    Gi1/4
15   DMZ                              active    Gi1/11, Gi1/14, Gi1/15, Gi1/16
19   SasVIDORES                       active    Gi2/2, Gi2/3, Gi2/5, Gi2/6,
Gi2/8, Gi2/10
20   INTERCONEXION_FW                 active
40   USUARIOS                         active    Gi3/10, Gi3/14, Gi3/15, Gi3/16,
Gi3/17, Gi3/19, Gi3/21, Gi3/24, Gi3/25, Gi3/27
45   VPN_zona-A                       active    Gi4/8, Gi4/11
1183 VPN_zona-B                       active


Configuración de una Interfaz del switch en modo "Promiscuo" para capturar el
tráfico de todas las tramas del switch.


Ejemplo-SW_ACE#sh monitor
Session 1
---------
Type                   : Service Module Session
Modules allowed        : 1-9
Modules active         : 4
BPDUs allowed          : Yes
```

```
Session 2
---------
Type                    : Local Session
Source VLANs            :
    Both                : 19
Destination Ports       : Gi4/8

Ejemplo-SW_ACE#sh run int g4/8
Building configuration...
Current configuration : 115 bytes
!
interface GigabitEthernet4/8
 description usuarios:GIG4/2:PROMISCUO
 no ip address
 load-interval 30
end
```

NOTA: en todos los párrafos anteriores, hemos presentado el concepto y las configuraciones de VLAN de nivel 2. Tal cual hemos ya comentado, los dispositivos actualmente para ofrecer mejores prestaciones suelen no respetar la idea del modelo de capas y abarcar más de una de ellas, con los switch de alta gama en general es frecuente la configuración de VLAN de nivel 2 y también VLAN de nivel 3 (*recordemos que el concepto de "switch" es un dispositivo que debería operar en nivel 2*), una VLAN de nivel 3 se distingue claramente pues se le asigna una dirección IP en su configuración, pero este tema lo desarrollaremos más adelante cuando tratemos el nivel 3 "Routing".

Para seguir analizando e investigando proponemos la descarga desde la Web www.darFe.es de las capturas que detallamos a continuación y hacer uso del analizador de protocolos (**Wireshark**):

- o 802-1q_01.pcap
- o 802-1q_02.pcap:

4.2.4. MPLS (Multiprotocol Label Switching).

Debido a las limitaciones del switching VLAN para grandes redes, se fue imponiendo una tecnología más flexible y de fácil expansión, apareciendo **VPLS** (Virtual Private LAN Service). Se da servicio Ethernet (Nivel 2) sobre una red IP/MPLS.

VPLS es la mejor forma de expandir redes Ethernet "multipunto a multipunto" integrando la tecnología IP con MPLS. La gran ventaja es que expande las redes LAN Ethernet a extensas regiones geográficas. Si bien existen diferentes formas de implementarlas, en este texto nos centraremos en Ethernet sobre MPLS.

Ventajas:

- Escalabilidad: No existe el límite de 4096 VLANs.
- Se elimina STP.
- Se puede proporcionar QoS.

- Se puede hacer ingeniería de tráfico.

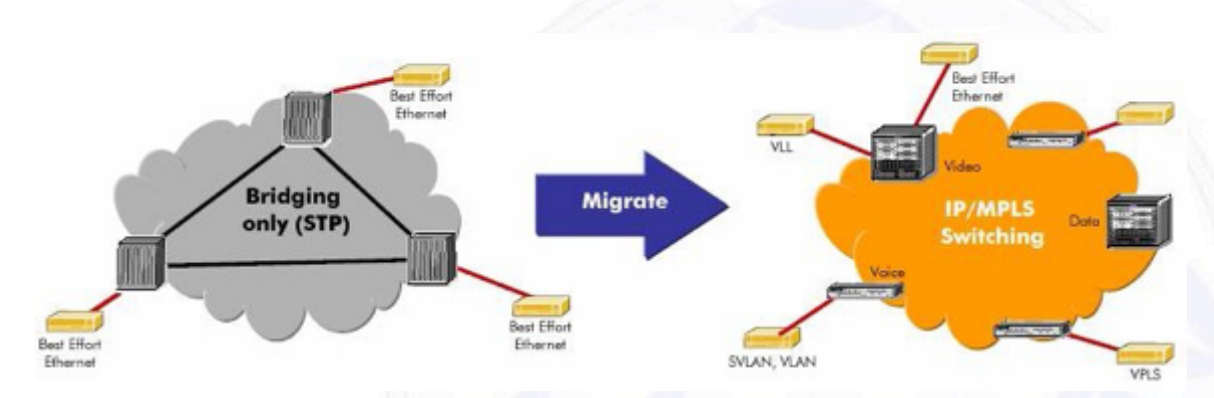


Imagen 4.4 (Diferencias entre VLAN e IP/MPLS)

El aspecto que destaca y mejora la velocidad de MPLS es el concepto de "Switching". En la jerga de telecomunicaciones, con esta palabra ya suena a nivel de enlace, y eso es justamente de lo que se trata el mismo: conmutar por medio del valor de estas etiquetas (labels) entre routers que hablen este protocolo.

Todo router que tenga la capacidad de trabajar con MPLS y que así esté configurado se denomina: Label Switch Router (**LSR**) y tenemos tres tipos de ellos:

1) Ingress LSRs: recibe un paquete que no ha sido etiquetado aún, inserta un etiquetado (stack) en el paquete y lo envía.
2) Eggress LSRs: recibe paquetes etiquetados, quita las etiquetas, y envía el paquete.
3) Intermediate LSRs: recibe un paquete etiquetado entrante, realiza un operación sobre este, conmuta el paquete y lo envía (sin tocar ninguna etiqueta).

En el protocolo MPLS es común referirse a este tipo de routers como Router "**P**" (Provider) y routers "**PE**" (Provider Edge). Un router P (o router Proveedor) es un Label Switch Router (LSR) que funciona como un router de tránsito de la red principal. El router P típicamente está conectado a uno o más enrutadores de PE. De forma práctica, es útil hacerse a la idea que un router PE (Edge), como su nombre lo indica, es la frontera de una red MPLS, por lo tanto son los que "etiquetarán" o "des etiquetarán" paquetes IP y lo introducirán o sacarán de la red MPLS; en cambio los routers "P" son el verdadero corazón de la red MPLS y serán los responsables de "conmutar" o ejecutar las tareas de "tránsito" de estos paquetes previamente etiquetados.

El término router PE define un equipo capaz de soportar una amplia gama de protocolos de enrutamiento, en particular:

- Border Gateway Protocol (**BGP**)
- Open Shortest Path First (**OSPF**)

- Multi-Protocol Label Switching (**MPLS**)

Los routers PE no tienen que ser conscientes de qué tipo de tráfico proviene de la red del proveedor.

Con MPLS un router de cliente, llamado **CE** (custormer Edge), hace peer IP con al menos un Router del proveedor llamado **PE**. Es decir que el router PE debe tener al menos una interfaz del lado de nuestra red (Proveedor) y al menos otra del lado del cliente (CE).

Este diálogo entre cliente y proveedor es importante pues a ningún cliente le interesa que sus datos puedan ser accesibles por otro cliente, por esta razón la privacidad en una red MPLS es lograda a través de **VRF** (Virtual Routing Forwarding) que ya mencionamos con anterioridad. VRF asegura que la información de enrutamiento de los clientes diferentes es mantenida de manera separada, y la red MPLS en el backbone asegura que los paquetes sean enviados en base a la información de etiqueta y no en base a la dirección IP.

La implementación mas popular de MPLS es **MPLS-VPN** (Virtual Private Network) en la cual los router PE que se encuentran entre la red del cliente y la red del proveedor de servicio levantan una conexión VPN con el PE del site remoto del cliente, así los router P no tienen que conocer ese trafico. Para lo anterior, se necesita que en los PE ya sean configurados los parámetros: Route distinguisher (**RD**), route targets (**RT**), y el envío de paquetes etiquetados dentro del la red MPLS.

El **RD tiene un solo propósito**: hacer prefijos IPv4 globalmente únicos. No se utiliza para el reenvío de paquetes IP (en routers del núcleo MPLS), pero es utilizado por los routers de borde para identificar a qué VPN pertenece un paquete. . El route target (**RT**) indica los miembros de una VPN y facilita la importación y exportación de VPNs dentro o fuera de nuestras VRFs. El RT funciona como una política de enrutado, ya que determina como se distribuyen las rutas de una VPN particular.

Un ejemplo puede ser:

```
Router_ACE
vrf definition vrf100
rd 65000:100
!
address-family ipv4
route-target export 65000:100
route-target import 65000:100
exit-address-family
¡
```

En cuanto a VRF, cada PE tendrá una instancia VRF por cada VPN que posea. El PE tendrá una tabla de enrutamiento por cada VRF y una tabla de enrutamiento global de direccionamiento IP.

Para crear cada VRF se usa "***#ip vrf***" y para asociar una interfaz a cada vrf se usa "***#ip vrf forwarding***", una interfaz solo puede ser parte de un solo VRF. Este detalle para nosotros es muy importante, pues en definitiva es el parámetro que nos asegura que se está separando adecuadamente el tráfico de cada usuario, y que a su vez para cada uno de esos usuarios nuestra red será absolutamente transparente, pues no tienen posibilidad de "ver" la traza de cada uno de esos saltos, la información se encuentra dentro de una especie de túnel con una única entrada y salida, determinada por únicas dos interfaces concretas desde donde se configuró "#ip_vrf". Los paquetes son etiquetados y enviados con una etiqueta desde el ingress PE router al egress PE router, y cada uno los router intermedios sólo pueden reconocer la "etiqueta" (label) que está por debajo de ese paquete IP, por lo tanto no se ven estas direcciones IP. Cuando la VRF debe ser importada (a la salida de MPLS) por ejemplo a BGP, aquí es donde entran en juego los parámetros Route distinguisher (RD), route targets (RT) que mencionamos antes y que extienden esta VPN hasta donde se desee.

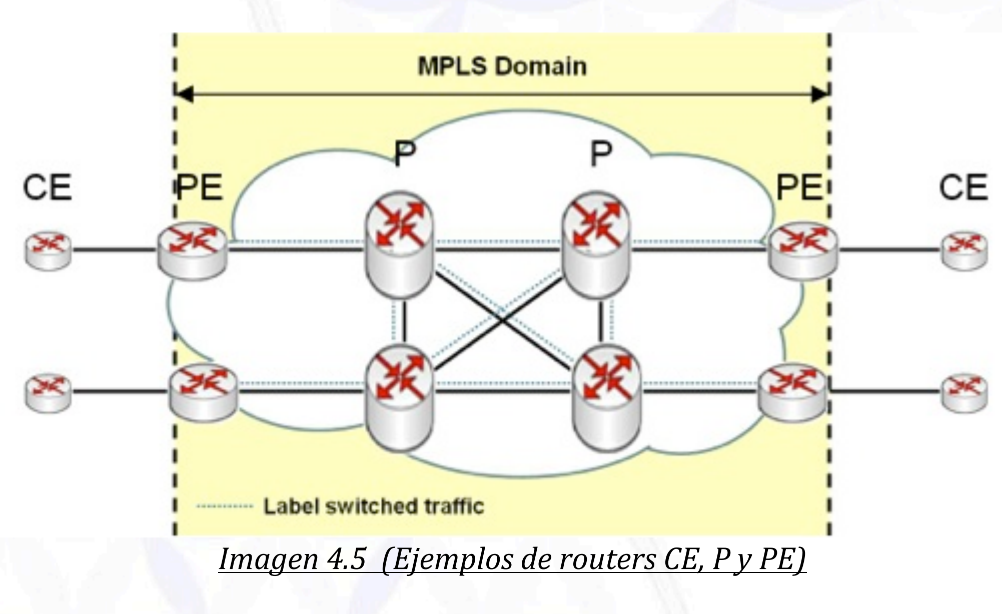


Imagen 4.5 (Ejemplos de routers CE, P y PE)

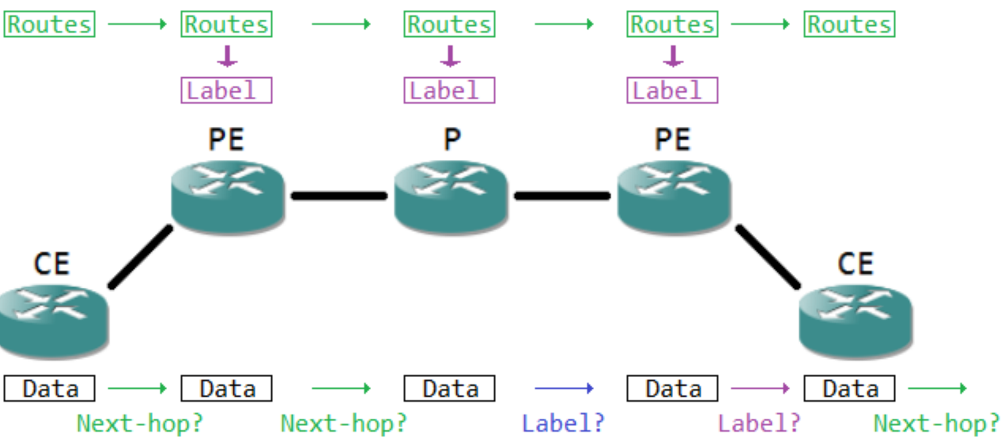


Imagen4.6 (Ejemplo de etiquetas)

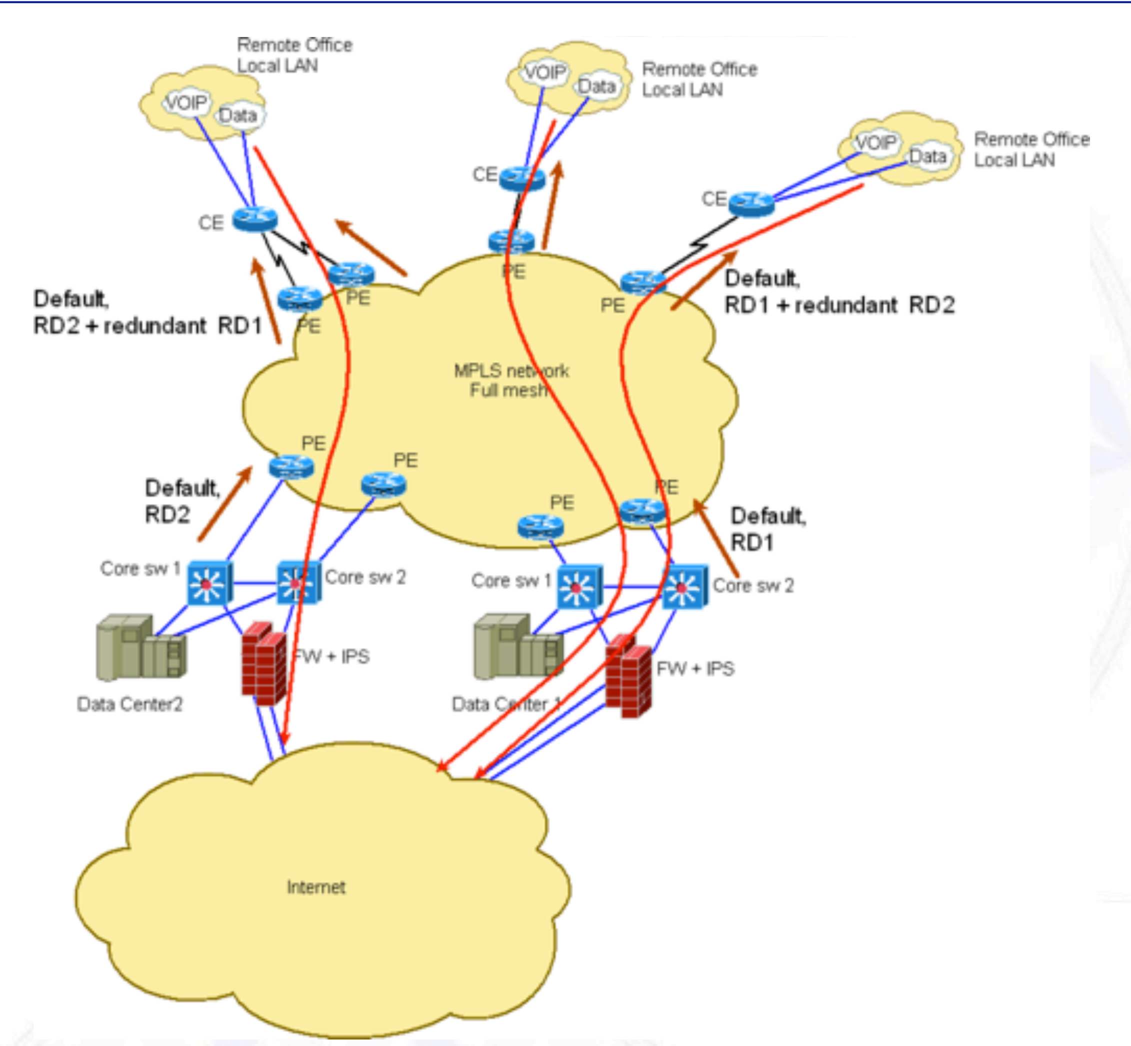


Imagen 4.7 (Ejemplo de extensión de la VPN de los router PE, a través del RD)

Si bien aún estamos en el nivel 2, MPLS también podemos presentarlo desde el nivel 3, pues con la difusión del protocolo IP, surgió la cuestión de qué tecnología o protocolo sería óptima para transportar los paquetes generados por la capa de red bajo protocolo IP, (*en particular hoy en día que contienen múltiples tipos de tráfico (voz, video, datos, etc.*). IP está diseñado para trabajar sobre una gran variedad de protocolos en la capa de enlace (nivel 2), Ethernet, Token Ring, **HDLC** ("High Level Data Link Control") o **ATM** (asychronous Transfer Mode), estos se encuentran desarrollados en el libro "**Seguridad por Niveles**" .

Sobre estos conceptos es que se desarrollaron diferentes alternativas:

- IP sobre SDH (IP/SDH).
- IP sobre ATM (IP/ATM)
- IP sobre TDM (IP/TDM) (**TDM**: Multiplexación por división de Tiempo)
- IP sobre Ethernet (IP/Ethernet)

Cada una de ellas presenta sus ventajas y desventajas. ATM ya está prácticamente en desuso y fue desbordado totalmente por las altas e inimaginables

velocidades alcanzadas por Ethernet. TDM es orientado a conexión (ventajas para QoS) y Ethernet no, pero una vez más, la velocidad ha ganado la partida con el desarrollo y optimización de best-effort, hay factores de flexibilidad, escalabilidad y eficiencia que hacen que el mundo se haya decantado por la última de las opciones, y bajo esta idea en definitiva, nació a mediados de los años 90 MPLS, que a decir verdad, en su momento no mereció el reconocimiento como mejor protocolo capaz de unir los mundos de conmutación de paquetes y la de circuitos, pudiendo crear circuitos virtuales (*como en ATM o Frame Relay*) utilizando etiquetas añadidas a los paquetes IP, pero en estos días sí ha sido valorado y es casi omnipresente en todas las grandes redes que poseen amplia distribución geográfica.

En cuanto a la posición que ocuparía en la pila de protocolos OSI o TCP/IP, inicialmente se plantearon dos propuestas de etiquetamiento, en nivel 3 o en nivel 2. La opción del nivel 2 resultó más interesante porque lo independizaba del nivel de red y además permitía ejecutar una conmutación más rápida pues se debería desencapsular un nivel menos. Conceptualmente, se optó por presentar a MPLS en una capa intermedia entre ambas:

Propiedades de MPLS.

- Proporciona Calidad de Servicio (QoS).

  A través de los diferentes Path puede ofrecer ciertas garantías de QoS permitiendo reservar ancho de banda para dicho tráfico en los enlaces que componen esos caminos o LSPs

- Incluye gestión o ingeniería de tráfico

  Con MPLS se pueden planificar rutas de extremo a extremo, de forma manual, en base a previsiones y estimaciones a largo plazo con el fin de optimizar los recursos y reducir congestión.

- Ofrece conmutación de alta velocidad

  Gracias al empleo de etiquetas, toda la información de rutas viaja en nivel 2 sin mirar el protocolo IP del paquete original IP, lo que agiliza la conmutación.

- Robustez y recuperación ante desastres

  Su topología de "multipunto a multipunto" ofrece la flexibilidad para desviar tráfico sobre la marcha en caso de fallo de enlaces y congestión de red.

  Los servicios basados en MPLS permiten conectar los dispositivos a través de múltiples conexiones redundantes a la nube MPLS.

- MPLS permite transportar todo tipo de servicios

  Como hemos mencionado al principio, MPLS funciona sobre todo tipo de tecnologías de nivel de enlace: ATM, Frame Relay, Ethernet, etc. Por lo tanto sobre MPLS puede viajar cualquier otro protocolo de nivel superior.

- Es compatible con procedimientos de las redes IP en cuanto a operación, mantenimiento y gestión.

  Cualquier router P o PE puede ser configurado para responder a los comandos típicos de gestión de red, habitualmente llamado "TroubleShooting", como por ejemplo: Ping, TraceRoute, snmp, etc. A su vez las interfaces realizan descubrimiento de enlaces, monitorización y supervisión e indicación de fallos en remoto.

- Soporta múltiples redes privadas virtuales (VPNs)

  Como mencionamos, cada VPN está relacionada a un LSP diferente, y es posible reservar diferente ancho de banda para cada una de ellas.

- Escalabilidad

  Las etiquetas pueden anidarse y cada nivel de la pila de etiquetas define diferentes LSPs, de esta manera dentro de una red MPLS se establece una jerarquía de LSPs que puede escalarse cuanto se desee.

4.2.5. 802.1x Autenticación de dispositivos conectados a un puerto LAN.

802.1x es una norma para incrementar el control de accesos. Básicamente propone un dispositivo que hace las veces de "puerta de acceso" que por defecto está siempre **cerrada**, al hacerse presente un elemento que desea acceder (*suplicante*), el dispositivo que recibe esta petición (y que reiteramos, tiene su puerta cerrada), realiza las veces de "pasarela" enrutando esta petición hacia el dispositivo responsable de la "*Autenticación*" (LDAP, RADIUS; Kerberos, etc.), el mecanismo o algoritmo de autenticación puede operar de diferentes formas (que desarrollaremos en este punto) pero en definitiva, luego del diálogo de autenticación, si la misma es válida, entonces recién allí "abre su puerta" de acceso. Este protocolo puede ser empleado tanto en redes cableadas, como en redes inalámbricas y opera en el nivel 2 que es aún el foco de este capítulo.

Desde el punto de vista de seguridad de una red LAN, **no puede ser dejado de lado**, al menos en su análisis y mínima configuración, y es altamente recomendable su implementación pues hoy en día cualquier switch o punto de acceso programable de gama media ya incorpora este protocolo.

Para el desarrollo de este capítulo tomaremos como referencia dos normas, la primera de ellas es:

- **IEEE Std 802.1x - 2010** ("Port-Based Network Access Control": **PBNAC**)

Y la segunda:

- **IEEE Std 802.1Xbx - 2014** ("Port-Based Network Access Control. Amendment 1: MAC Security Key Agreement Protocol (**MKA**) Extensions"), *que es la primera enmienda sobre la del 2010 mencionada.*

Lo primero que se establece en estas normas es que PBNAC permite a un administrador de red restringir el uso de los puntos de acceso a los servicios de una LAN que responda a la familia IEEE 802 asegurando la autenticación y el control de acceso a los dispositivos. Este estándar especifica el uso del Protocolo de Autenticación Extensible (**EAP**: Extensible Authentication Protocol) regulado por la **RFC-3748** para el proceso de autenticación, encapsulándolo sobre los protocolos de LAN, por lo que se conoce como **EAPOL** (EAP Over LAN)

El esquema básico (*hay varios más*) de conexión que propone esta norma es el que se presenta en la misma como "***Figure 7-6*** *- Network access control with MACsec and a point-to-point LAN*" dentro de la misma y que pegamos a continuación:

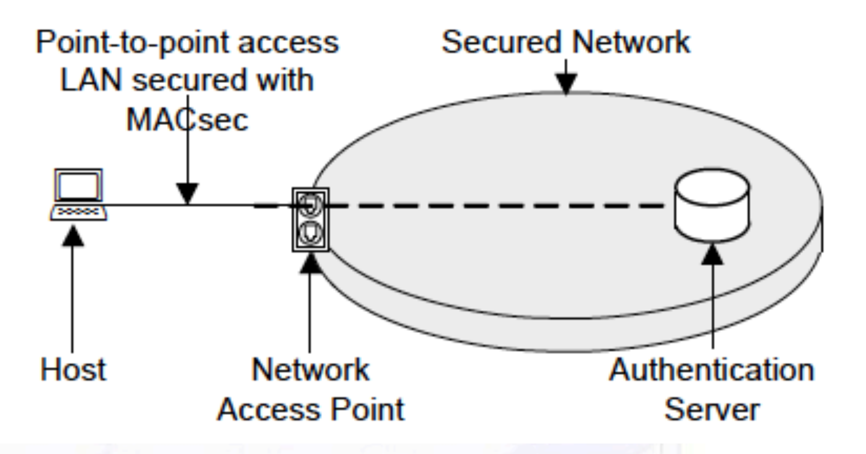


Imagen 4.8 (Figura tomada de la norma IEEE 802.1x – 2010)

En la imagen anterior podemos identificar tres dispositivos: host, Network Access Point y Authentication Server que serán las piezas de esta arquitectura.

Antes de seguir avanzando, deseamos presentar tres normas más sobre las que se basa todo el proceso de autenticación soportado por 802.1x, las mismas no serán desarrolladas en este texto, pero hemos considerado importante mencionarlas para quien desee profundizar sobre las mismas, estas son:

- **IEEE Std 802.1AE-2006** (IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security).

- **IEEE Std 802.1AR** (IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identifier).
- **IEEE Std 802.1AX** (IEEE Standard for Local and Metropolitan Area Networks: Link Aggregation).

Volviendo al estándar 802.1x, elpróximo punto que describiremos brevemente es "5.3 Componentes del sistema". Aquí nos presenta que un sistema que incorpore 802.1x debe estar compuesto por 2 entidades:

a) <u>Port Access Entity</u> (**PAE**)

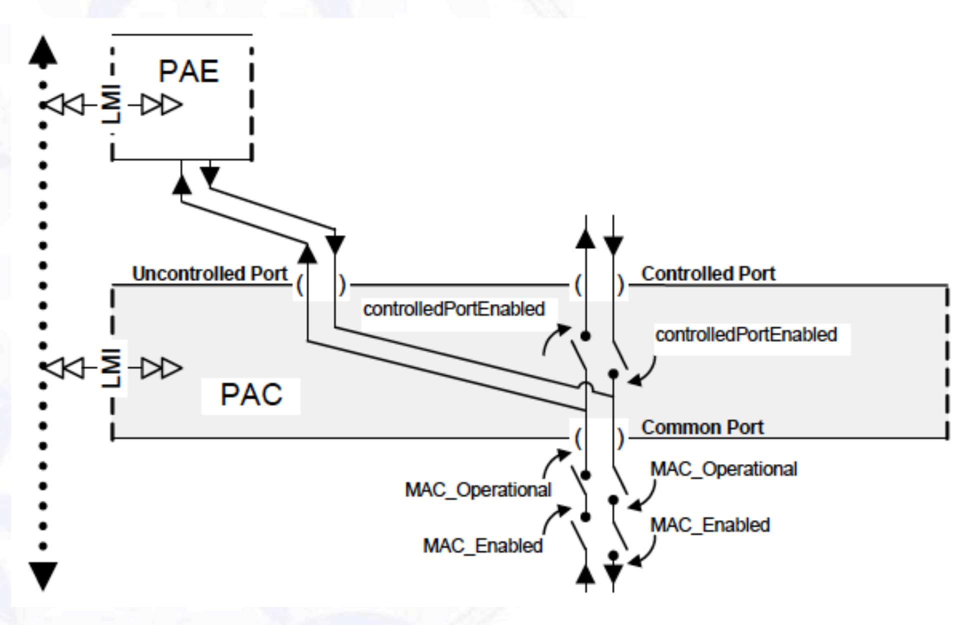
El concepto de PAE, podríamos definirlo como una "<u>Entidad</u>" (algo abstracto) pero que en la práctica se ve reflejado en las funciones que desempeña. Un puerto para que opere en conformidad con esta norma debe incorporar al menos una de las siguientes "<u>funciones</u>" de PAE:

- Supplicant
- Authenticator
- MACsec Key Agreement (MKA)

Cada una de estas funciones está descripta en el punto 6.3 de la norma

b) <u>Port Access Controller</u> (**PAC**)

El PAC es la entidad que provee el <u>control del puerto</u>, las decisiones las adopta el PAE pero la acción concreta es la función del PAC. Este diálogo entre la decisión y la apertura del puerto se lleva a cabo mediante una variable denominada "*ControlledPortEnable*", la cual opera como un conmutador físico "normal abierto" y la podemos ver en siguiente figura:



<u>Imagen 4.9 (Figura tomada de la norma IEEE 802.1x – 2010)</u>

Otro punto sobre el que merece la pena detenernos es el punto "*6. Principles of port-based network access control operation*" PBNAC permite a lso administradores de la red restringir su uso mediante el "Servicio de Punto de Acceso de Puertos" (ports*service access points*) asegurando la comunicación con sistemas autenticados y autorizados , estas cláusulas especifican lo siguiente:

a) Funciones ejecutadas por sistemas que soporten PBNAC (*lo desarrolla en el punto 6.1*).
b) LA jerarquía de claves empleada para asegurar la comunicación (*lo desarrolla en el punto 6.2*).
c) La entidad PAE (*lo desarrolla en el punto 6.3*) que puede:
   - Usar EAP para proveer autenticación mutua.
   - Soporte para la configuración de "pre-shared keys" (PSKs) para soportar autenticación mutua.
   - Soporte para el uso de identidad de dispositivos, según lo establece IEEE 802.1AR, para soportar autenticación mutua.
   - Identificación de redes y gestión de claves usando roaming.
   - Acuerdos con los requerimientos que especifica IEEE 802.1AE

Tal cual hemos mencionado al principio, uno de los factores clave de 802.1x es el empleo de EAP (si bien soporta el empleo de PSK: Pre Shared Key), tema que describe la norma en el punto "*8. Authentication using EAP*". Este protocolo puede ser usado para la autenticación mutua entre el "suplicante" PAE (Port Access Entity) y el "autenticador" PAE cada uno de ellos conectados a un puerto físico de LAN. EAP a su vez soporta diferentes mecanismos de autenticación incluyendo Kerberos, empleo de clave pública, One time passwords. El autenticador a su vez debe soportar **AAA** (Autentication, Autorization y Accounting).

Cada PAE implementa el Protocolo de control de acceso a puerto (**PACP**: Port Access Control Protocol) y a su vez un método de nivel superior para la Autenticación, que es quien provee EAP. Aquí notamos una diferencia práctica, pues el nivel superior del PAE suplicante solo aplica EAP, el del Autenticador lo hará para authentication, authorization, and accounting (AAA) y entre ambos el resultado solo pueden ser tres opciones "Success", "fail" o "time out". Las especificaciones de nivel superior no se encuentran dentro del ámbito de esta norma, pero para avanzar a título de ejemplo, en este texto desarrollaremos cómo opera **EAP-TLS** (regulado por la **RFC-5216**) en su integración con IEEE 802.1AR y veremos el diálogo entre un "Suplicant" y un "Autenticator"

A continuación, presentamos una secuencia de autenticación empleando EAP-TLS.

No.	Time	Source	Destination	Length	Protocol	Info
99	16:28:46.013550	00:24:51:17:63:8c	01:80:c2:00:00:03	60	EAP	Request, Identity
101	16:28:46.201542	00:24:51:17:63:8c	01:80:c2:00:00:03	60	EAP	Request, Identity
102	16:28:46.202114	3c:07:54:6c:a2:29	01:80:c2:00:00:03	36	EAP	Response, Identity
112	16:28:48.385759	00:24:51:17:63:8c	01:80:c2:00:00:03	60	EAP	Request, Protected EAP (EAP-PEAP)
113	16:28:48.388846	3c:07:54:6c:a2:29	01:80:c2:00:00:03	150	TLSv1	Client Hello
114	16:28:48.397336	00:24:51:17:63:8c	01:80:c2:00:00:03	1514	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done
115	16:28:48.397542	3c:07:54:6c:a2:29	01:80:c2:00:00:03	24	EAP	Response, Protected EAP (EAP-PEAP)
116	16:28:48.405827	00:24:51:17:63:8c	01:80:c2:00:00:03	1514	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done
117	16:28:48.405974	3c:07:54:6c:a2:29	01:80:c2:00:00:03	24	EAP	Response, Protected EAP (EAP-PEAP)
118	16:28:48.414438	00:24:51:17:63:8c	01:80:c2:00:00:03	1514	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done
119	16:28:48.414565	3c:07:54:6c:a2:29	01:80:c2:00:00:03	24	EAP	Response, Protected EAP (EAP-PEAP)
120	16:28:48.430284	00:24:51:17:63:8c	01:80:c2:00:00:03	594	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done
121	16:28:48.431183	3c:07:54:6c:a2:29	01:80:c2:00:00:03	222	TLSv1	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Hands…
122	16:28:48.442948	00:24:51:17:63:8c	01:80:c2:00:00:03	71	TLSv1	Change Cipher Spec, Encrypted Handshake Message
123	16:28:48.459674	3c:07:54:6c:a2:29	01:80:c2:00:00:03	24	EAP	Response, Protected EAP (EAP-PEAP)
124	16:28:48.471690	00:24:51:17:63:8c	01:80:c2:00:00:03	60	TLSv1	Application Data
125	16:28:48.472068	3c:07:54:6c:a2:29	01:80:c2:00:00:03	59	TLSv1	Application Data

imagen 4.10 (Captura de tráfico 802.1x)

En la secuencia de tramas de la imagen anterior está filtrado únicamente el tráfico EAP, podemos ver tres direcciones MAC, la que finaliza en "**.29**" se corresponde con el "PAE Suplicant" (*En este ejemplo se trata de mi propio ordenador Portátil*), la que finaliza con "**.8c**" es el "PAE Autenticator", y la que finaliza con "**.03**" es el PAC. Si esta misma captura la deseamos analizar como componentes físicos, serían el "host", el "AAA" y el "Access Point" respectivamente.

Si seguimos avanzando en esta captura podemos desplegar una de esas tramas (*en el ejemplo que sigue es la trama nº 101 de la imagen anterior*).

Frame 101: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: 00:24:51:17:63:8c, Dst: 01:80:c2:00:00:03
  Destination: **01:80:c2:00:00:03**
  Source: **00:24:51:17:63:8c**
  Type: 802.1X Authentication (0x**888e**)
  Padding: 000000000000000000000000000000000000000000000...
802.1X Authentication
  Version: **802.1X-2010** (3)
  Type: **EAP Packet** (0)
  Length: 5
  Extensible Authentication Protocol
    Code: **Request** (1)
    Id: 1
    Length: 5
    Type: Identity (1)
    Identity:

De la captura desplegada podemos ver que este diálogo es desde el PAE Autenticator (**00:24:51:17:63:8c**), hacia el PAC (**01:80:c2:00:00:03**).

Por ahora nos interesa sólo los campos que hemos resaltado en negrita. Vemos que en el parámetro "Ethertype" del encabezado Ethernet aparece el valor (0x**888e**) lo que identifica que se trata de una trama 802.1x. Una vez que nos metemos en el encabezado 802.1x, se aprecia el valor Version: **802.1X-2010** (3) que no sindica que estamos hablando justamente de la versión de la norma que estamos tratando en este

texto, luego el Type: **EAP Packet** (0) con su valor "0" nos hacer referencia a que emplearemos EAP y por último que se trata de una solicitud Code: **Request** (1).

A continuación presentamos a respuesta a esta solicitud:

```
Frame 102: 36 bytes on wire (288 bits), 36 bytes captured (288 bits) on interface 0
Ethernet II, Src: 3c:07:54:6c:a2:29, Dst: 01:80:c2:00:00:03
  Destination: 01:80:c2:00:00:03
  Source: 3c:07:54:6c:a2:29
  Type: 802.1X Authentication (0x888e)
802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: EAP Packet (0)
  Length: 18
  Extensible Authentication Protocol
    Code: Response (2)
    Id: 1
    Length: 18
    Type: Identity (1)
    Identity: administrador
```

De la captura anterior, sólo deseamos destacar que se trata de una respuesta (Code: **Response** (2)), que va dirigida desde el "PAE Suplicant" (*mi propio ordenador Portátil:* Source: **3c:07:54:6c:a2:29**), hacia el PAC (**01:80:c2:00:00:03**), haciéndome presente en esta LAN como "Identity: **administrador**" pues ese es mi perfil local en la portátil.

Es importante que prestemos atención a este diálogo, pues como podemos ver, la comunicación (tal cual hemos visto en la *Figura tomada de la norma IEEE 802.1x*) no es directa desde mi MAC hasta la MAC del autenticador, sino que el envío y recepción de estas tramas se hace a través del **PAC** que obra como punto de control de acceso, sin permitirme pasar al interior de esta red, es decir, hasta ahora sólo tengo comunicación con la interfaz física: **01:80:c2:00:00:03** que en definitiva es la boca del switch al que estoy conectado, pero no puedo pasar de allí pues está "Cerrado".

A continuación presentamos las dos tramas que configuran cómo se establecerá la sesión TLS:

```
Frame 113: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
Ethernet II, Src: 3c:07:54:6c:a2:29, Dst: 01:80:c2:00:00:03
  Destination: 01:80:c2:00:00:03
  Source: 3c:07:54:6c:a2:29
  Type: 802.1X Authentication (0x888e)
802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: EAP Packet (0)
  Length: 132
  Extensible Authentication Protocol
    Code: Response (2)
    Id: 2
    Length: 132
```

Type: Protected EAP (EAP-PEAP) (25)
EAP-TLS Flags: 0x80
1... .... = Length Included: True
.0.. .... = More Fragments: False
..0. .... = Start: False
.... .000 = Version: 0
EAP-TLS Length: 122
Secure Sockets Layer
TLSv1 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 117
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 113
Version: TLS 1.0 (0x0301)
Random
GMT Unix Time: Jan 31, 2013 16:28:48.000000000 CET
Random Bytes: e6ad13c06f460241d0fecac186e3542a4f80d0ae5f89ef...
Session ID Length: 0
Cipher Suites Length: 54
Cipher Suites (27 suites)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
Cipher Suite: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
Cipher Suite: TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
Cipher Suite: TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
Cipher Suite: TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
Cipher Suite: TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
Compression Methods Length: 1
Compression Methods (1 method)

Compression Method: null (0)
Extensions Length: 18
Extension: elliptic_curves
Type: elliptic_curves (0x000a)
Length: 8
Elliptic Curves Length: 6
Elliptic curves (3 curves)
Extension: ec_point_formats
Type: ec_point_formats (0x000b)
Length: 2
EC point formats Length: 1
Elliptic curves point formats (1)

En la trama anterior destacamos que nuevamente se trata de una comunicación que va dirigida desde el "PAE Suplicant" (*mi propio ordenador Portátil:* Source: **3c:07:54:6c:a2:29**), hacia el PAC (**01:80:c2:00:00:03**), en la cual me presento para hacer uso de TLS "**EAP-TLS Flags: 0x80**"empleando la versión 1 del mismo "**TLSv1 Record Layer**" y que se trata de una solicitud de inicio cliente " **Handshake Protocol: Client Hello**", a continuación mi portátil hace presente toda la suite de protocolos de cifrado que está en capacidad de operar dentro de TLS "**Cipher Suites (27 suites)**", y dentro de esta hemos resaltado la que veremos a continuación (*en la trama 114*) selecciona el Autenticador como algoritmo de cifrado "**Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)**".

En la trama siguiente (114 de la imagen inicial) vemos la respuesta desde el PAE Autenticator (**00:24:51:17:63:8c**), hacia el PAC (**01:80:c2:00:00:03**).

Frame 114: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: 00:24:51:17:63:8c, Dst: 01:80:c2:00:00:03
802.1X Authentication
Version: 802.1X-2010 (3)
Type: EAP Packet (0)
Length: 1496
Extensible Authentication Protocol
Code: Request (1)
Id: 3
Length: 1496
Type: Protected EAP (EAP-PEAP) (25)
EAP-TLS Flags: 0xc0
1... .... = Length Included: True
.1.. .... = More Fragments: True
..0. .... = Start: False
.... .000 = Version: 0
EAP-TLS Length: 5036
[4 EAP-TLS Fragments (5036 bytes): #114(1486), #116(1490), #118(1490), #120(570)]
Secure Sockets Layer
TLSv1 Record Layer: Handshake Protocol: Multiple Handshake Messages
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)

Length: 5031
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 70
Version: TLS 1.0 (0x0301)
Random
GMT Unix Time: Jan 31, 2013 16:26:29.000000000 CET
Random Bytes:0d07e979d3e1b76dafb9cb7be976a9905fbdeffe7852a11
Session ID Length: 32
Session ID: 99010000ca36cdc8e9efa9702041c8741c49a2378c42655d...
Cipher Suite: **TLS_RSA_WITH_RC4_128_MD5 (0x0004)**
Compression Method: null (0)
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 1424
Certificates Length: 1421
Certificates (1421 bytes)
Certificate Length: 1418
Certificate:
308205863082046ea003020102020a2ded7dc70000000000... (id-at-commonName=w2003epo46.tfn.local)
signedCertificate
version: v3 (2)
serialNumber: 0x2ded7dc7000000000008
signature (sha1WithRSAEncryption)
issuer: rdnSequence (0)
validity
subject: rdnSequence (0)
subjectPublicKeyInfo
extensions: 8 items
algorithmIdentifier (sha1WithRSAEncryption)
Padding: 0
encrypted:
7458a256c0f33cc9905f18317343daf62e04a230b64de972...
Handshake Protocol: Certificate Request
Handshake Type: Certificate Request (13)
Length: 3521
Certificate types count: 2
Certificate types (2 types)
Certificate type: RSA Sign (1)
Certificate type: DSS Sign (2)
Distinguished Names Length: 3516
Distinguished Names (3516 bytes)
Handshake Protocol: Server Hello Done
Handshake Type: Server Hello Done (14)
Length: 0

De esta trama, por ahora sólo quedémonos con que el Autenticador selecciona el algoritmo de cifrado "Cipher Suite: **TLS_RSA_WITH_RC4_128_MD5 (0x0004)**" e inicia el diálogo para implementar TLS ofreciendo sus parámetros y

certificado digital que servirá para la generación de la integridad, confidencialidad, autenticación y control de acceso durante todo el proceso.

Todo este diálogo finalizará en nuestro ejemplo con una trama en la cual el Autenticador le Informa al PAC que el proceso ha tenido éxito, por lo tanto el PAC habilita el acceso de este puerto físico a mi portátil, este es la trama final del diálogo que presentamos a continuación:

Frame 142: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: 00:24:51:17:63:8c, Dst: 01:80:c2:00:00:03
  Destination: **01:80:c2:00:00:03**
  Source: **00:24:51:17:63:8c**
  Type: 802.1X Authentication (0x888e)
  Padding: 000000000000000000000000000000000000000000000...
802.1X Authentication
  Version: 802.1X-2010 (3)
  Type: EAP Packet (0)
  Length: 4
  Extensible Authentication Protocol
    Code: Success (3)
    Id: 11
    Length: 4

Todo este diálogo que acabamos de ver resumidamente en la práctica y con un ejemplo real es el que presenta esta norma en su imagen "*8.2 Autenticated-initated EAP-TLS (success)*" tal cual pegamos a continuación:

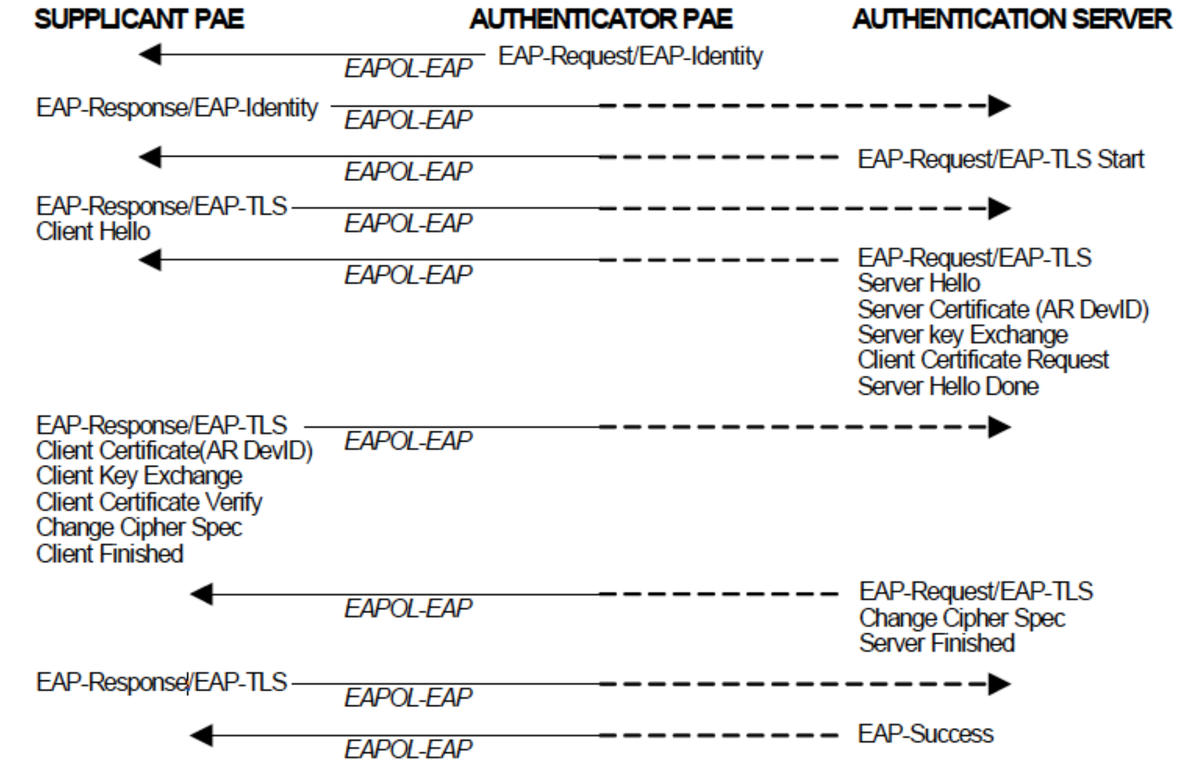


Figure 8-2—Authenticator-initiated EAP-TLS (success)

imagen 4.11 (Figura tomada de la norma IEEE 802.1x – 2010)

Toda la secuencia anteriormente presentada con un ejemplo real, es una de las formas de implementar 802.1x, la norma en sus 205 páginas presenta con todo detalle la metodología completa para incorporar este protocolo a nuestras LANs, pero no es objetivo de este libro ahondar tanto sobre la misma, sino solamente presentar la importancia que revista su puesta en producción como protocolo de nivel 2 para incrementar sensiblemente la seguridad de toda nuestra arquitectura de red.

4.2.6. IEEE 802.11 – Redes inalámbricas WLAN.

Este tema que es uno de los pilares actuales del nivel de enlace, y desde el punto de vista de la seguridad es fundamental tratar con máximo detalle, no lo desarrollaremos en este libro pues fue tratado desde el punto de vista de red y de seguridad en el capítulo 4 del libro "**Seguridad Por Niveles**", por lo tanto y par no ser redundantes, os invitamos a que recurráis a este otro libro para abordar el tema.

4.3. Controles de Seguridad básicos a implementar en un Switch

Siempre que se deseen considerar aspectos de seguridad en dispositivos, plataformas, bases de datos, sistemas operativos, etc. El mayor referente que debemos tener en cuenta se encuentra en las "**Guías CIS**" que publica el "**Center for Internet Security**" (https://www.cisecurity.org), rellenando el formulario de esta Web, nos permitirá descargar de forma gratuita todos los documentos de bastionado que presenta esta organización, los cuáles en algunos casos estarán más actualizados que otros, pero siempre son un pilar fundamental a considerar, su descarga la podemos realizar desde:

https://benchmarks.cisecurity.org/downloads/index.cfm

Haciendo un resumen de estas guía, las medidas mínimas de seguridad en un switch son (*nos centraremos particularmente en Cisco que son los que poseen la masa de las grandes redes, pero aplica también a cualquier otro*):

1) aspectos "Imprescindibles".
   a) Cerrar puertos/bocas no empleados (Download).
   b) Acceso vía SSH (no por telnet).

c) Configuración SNMP (versión 3): Para monitorizarlo

d) Configuración de Syslog (hacia servidor externo): Para envío hacia un servidor de Logs centralizado.

e) Configuración "ntp" (Network Time Protocol): Para sincronización de tiempos.

f) Activación de protocolo STP (Spanning Tree Protocolo) para evitar bucles.

g) Almacenamiento externo del archivo "running config": para poder recuperar su configuración.

2) Buenas prácticas.

a) Configuración de VLANs (Cuidado con las configuración de Trunk, protocolo VTP: Virtual Trunk Protocol [modos:Server, client y transparent]): para poder "segmentar" a nivel 2.

b) Empleo de protocolo 802.1q (si existen VLANs) (Cuidado con la VLAN Nativa: tráfico entre Switchs únicamente): Para hacer circular el tráfico de las VLANs por medio de este protocolo.

c) Verificación de empleo de "Port Mirroring" o SPAN (Switchport Analyzer): Para poder "espejar" el tráfico hacia un puerto determinado.

3) Detalles más específicos (que pueden ser recomendaciones de empleo).

a) Empleo de Protocolo 802.1x: Para habilitar el acceso a un puerto del switch por medio de un servidor adicional de autenticación (RADIUS, Kerberos)

b) Se pueden restringir las direcciones MAC que se pueden conectar a un puerto determinado (por Ej: el de gestión).

(ver o estudiar el comando: Switch(config-if)#switchport port-security)

Antes de entrar en el capítulo siguiente ("Routing"), insistiendo en la capacidad de los dispositivos actuales para realizar tareas de más de un nivel, presentamos la configuración de un "Switch" de la familia Cisco 6500, en este caso concretamente un Cisco 6506, cuya función principal es la de operar en nivel 2, pero con la característica que está configurado para operar también en nivel 3 (Routing). Este tipo de configuraciones las encontraremos con muchas frecuencia, pues son dispositivos muy potentes (y caros) que nos permiten por cada interfaz física decidir qué configuración deseamos darle y, tengamos en cuenta, que si podemos configurar diferentes VPNs y a su vez varias rutas IP, en definitiva estamos aprovechando en un solo dispositivo funciones que de otro modo nos implicaría adquirir varios switchs y varios routers, con un coste sensiblemente mayor.



El ejemplo que se presenta a continuación es una configuración real de un swich Cisco 6506 que opera en nivel 3 (y pos supuesto, también en nivel 2). Sobre esta configuración, iremos comentando línea a línea los aspectos fundamentales, dejando para más adelante el detalle de los parámetros relacionados a Routing que se tratarán en el capítulo siguiente.

```
R6506_Ejemplo#sho run

Building configuration...
Current configuration : 5925 bytes
!
! Last configuration change at 04:45:54 CDT Wed Sep 19 2016 by ace
! NVRAM config last updated at 04:50:23 CDT Wed Sep 19 2016 by ace
!
upgrade fpd auto
version 12.2
service tcp-keepalives-in
service tcp-keepalives-out
service password-encryption
service linenumber
service sequence-numbers
service counters max age 5
no service dhcp
!
hostname R6506_Ejemplo
!
logging snmp-authfail
logging buffered 32768 debugging
logging rate-limit all 1000
no logging console
enable secret 5 $1RzT$Gs.JGFc4medE311as
!
username ace privilege 15 secret 5 $1$bEN$$P5JcuTbsa45P3v1
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default enable
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local if-authenticated
aaa authorization commands 15 default group tacacs+ local if-authenticated
aaa accounting send stop-record authentication failure
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
```

Esta línea (*y la siguiente*) son importantes para el control de las conexiones TCP a través de telnet, SSH y vty. Corta la misma en caso de inactividad.

Mostrará la contraseña criptografiada.

Le espcecificamos qué deseamos que loguee.

Forzamos a ingresar una contraseña robusta para entrar en modo "privilegiado" (*administrador*). En los IOS actuales prevalece sobre otro comando que veremos con frecuencia que es "**enable password**"

Estos pasos definen la cuenta "ace", y cómo valida la misma contra TACACS para emplear AAA *(Authentication, Authorization y Accounting).*

…………..
….
..
no ip bootp server
!
ip vrf Gi_ACE
rd 24xx:3111
route-target export 24xx:3111
route-target import 24xx:3111
!
………
….
.
!
vlan 2
name VLAN POR DEFECTO
!
vlan 5
name GESTION_servicio
!
vlan 12
name GESTION_FWs
!
vlan 14
name SasVas_correo
!
vlan 21
name INTasNA
!
………
…
.
interface TUNEL_GESTION
description GESTION_RED
no ip address
tunnel source Loopback0
tunnel destination 10.10.37.22
tunnel mode eon
clns enable
!
interface Loopback0
description INTasFAZ GESTION
ip address 10.22.12.20 255.255.255.255
ip router isis
!
interface GigabitEthernet1/1
description SWITCH_NIVEL-3

Niega la posibilidad de arranque con protocolo "bootp" (*precursor de DHCP)*

Aquí vemos claramente que se trata de un "router **PE**" (*recordemos el* ***RD****: Route Distinguisher que presentamos en MPLS*), se está comenzando con la asociación de VPNs a VRFs , para luego poder emplear MPLS

Aquí sí vemos una clara función de nivel dos, donde se van definiendo las diferentes VLANs

Esta es la creación de un túnel sobre una interfaz de loopback, sin embargo vemos que la misma no tiene asignada dirección IP

Aquí sí se trata de una interfaz que trabaja en nivel 3 (*podemos ver que la misma tiene asignada una dirección IP*)

Por el contrario, aquí vemos una interfaz típica de nivel 2, con encapsulamiento 802.1q (*dot1q*) y que opera en modo "trunk".

```
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 logging event link-status
!
interface GigabitEthernet1/2
 description RED_INTasNA
 switchport
 switchport access vlan 21
 switchport mode access
 logging event link-status
 logging event spanning-tree status
!
…………
….
.
interface GigabitEthernet2/1
 description ENLACE_RED2
 mtu 1600
 ip address 10.22.12.5 255.255.255.252
 ip router isis
 mls qos trust dscp
 mpls label protocol ldp
 mpls ip
 clns router isis
 isis network point-to-point
……
…
.
!
interface Vlan2
 description VLAN POR DEFECTO
 ip address 10.22.12.10 255.255.255.224
 ip router isis
 clns router isis
!
interface Vlan14
 description SasVas_CORREO
 ip address 10.22.12.8 255.255.255.128
 ip router isis
 standby 10 ip 10.22.12.6
 standby 10 priority 110
 standby 10 preempt
 clns router isis
……..
….
.
```

Aquí vemos nuevamente una interfaz típica de nivel 2, que está asignada exclusivamente a la VLAN 21 y por alguna razón loguea ciertos eventos.

```
ip classless
ip route 0.0.0.0 0.0.0.0 10.22.12.7
ip route 10.20.29.10 255.255.255.255 10.22.10.7 name SEDE_2
ip route 10.20.29.9 255.255.255.255 10.22.10.7 name SEDE_3
……………
……
.
ip route vrf Gi_FW 10.22.12.25 255.255.255.255 10.22.12.66 name Fortinet_01
ip route vrf VPN100 0.0.0.0 0.0.0.0 10.22.12.22 name SALIDA_Internet
………
…
.
logging history size 30
logging trap notifications
logging source-interface Loopback0
logging 10.22.16.6
logging 10.22.17.6
access-list 10 permit 10.22.12.16
access-list 10 permit 10.22.21.2
access-list 94 permit 10.12.3.22
………
…
.
access-list 10 permit tcp host 10.12.1.8 host 10.22.12.9 eq www
access-list 10 permit tcp host 10.12.10.7 host 10.22.12.8 eq www
access-list 10 permit tcp host 10.22.13.22 host 10.22.13.100 eq ftp
access-list 10 deny ip any any
………
…
.
!
snmp-server community pruebasnmp22 RO 96
snmp-server trap-source Loopback0
snmp-server location SEDE1-SALA.10
snmp-server contact ace@ace.es
snmp-server enable traps isis
snmp-server enable traps config
snmp-server host 10.22.16.3
snmp-server host 10.22.17.4
tacacs-server host 10.15.1.2 key 7 12AAD151140D1453EE53
tacacs-server host 10.15.30.28 key 7 12AAD151140D1453EE53
!
line con 0
 transport output ssh
 stopbits 1
line vty 0 4
 access-class 94 in
```

En este acso vemos la definición de rutas estáticas (*pues está operando en nivel 3*).

Definiciones para Log de eventos y servidores de Logging

Aquí vemos la definición de las ACLs básicas *(solo operan a nivel 3).*

Aquí vemos la definición de las ACLs **extendidas** *(ya operan a nivel 4: puertos TCP 80 y 20/21).*

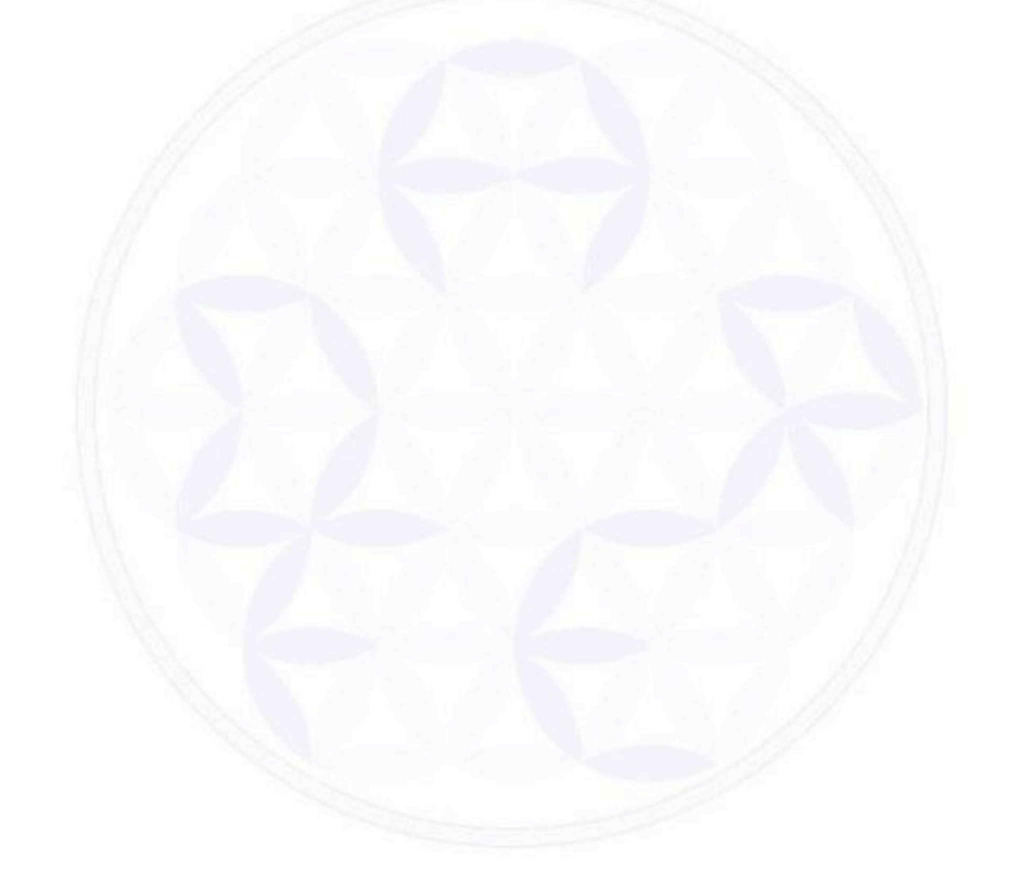
Definición del empleo de **SNMP** (*Single Network Monitor Protocol*). En este caso vemos que no figura el empleo de la versión 3 del mismo, por lo tanto este dispositivo usará version 1

Definición de los servidores de AAA *(Más adelante veremos el tema de Password 7)*

Definición de la línea de consola (*acceso físico por línea de gestión*) y las terminales virtuales (vty).

```
 transport input ssh
 transport output ssh
line vty 5 15
 access-class 94 in
 transport input ssh
 transport output ssh
ntp clock-period 17180156
ntp source Loopback0
ntp update-calendar
ntp server 10.222.120.229
ntp server 10.222.120.230
!
end
```

Definición de los servidores de tiempo y el empleo de NTP



5. Routing

5.1. Presentación

En el capítulo 5 del libro "**Seguridad por Niveles**" hemos desarrollado todos los conceptos relacionados al protocolo IP que es el núcleo del nivel de red, por eso aquí ya no nos detendremos en ello ,sino que abordaremos esta capa desde el punto de vista de las medidas de seguridad que debemos considerar para fortalecer los dispositivos encargados de gestionar el nivel 3. El dispositivo por excelencia en la pila TCP/IP de este capítulo es el "Router" cuya misión fundamental es el manejo de las "rutas" IP y su capacidad de conmutación de paquetes a través de la red, siempre basado en el encabezado del protocolo IP, toda esta tarea es la que denominaremos routing. Como ya nos ha sucedido varias veces, esta vez tampoco es la excepción, y veremos que los routers actuales tiene capacidad de abordar también funciones de otras capas de la pila TCP/IP que superan la actividad de routing, en estos casos también nos detendremos aunque exceda este concepto.

5.2. Definición de Routers

Para ejecutar la técnica de "Conmutación de paquetes", el único elemento de juicio que se tiene para ello, es el campo "Destination Address" del encabezado IP de cada paquete que le llega (no existe otro). En la configuración de cualquier dispositivo de red se poseen más datos, como son las máscaras de red, las interfaces, los protocolos de enrutado (estáticos o dinámicos) las rutas que conoce y las que no, el o los Gateway, las prioridades o no que debe darle a un paquete, etc. Toda esta serie de parámetros serán los que un Router es capaz de controlar de forma nativa

Con lo descripto resumidamente, acaban las funciones nativas de un router. Como hemos mencionado, comienzan a aparecer funcionalidades o servicios adicionales, pero lo importante es tener claro que esto es un "valor agregado" en un router, su función básica y primordial es la de: Enrutar.

Un router opera siempre en el nivel 3 (red) del modelo de capas:

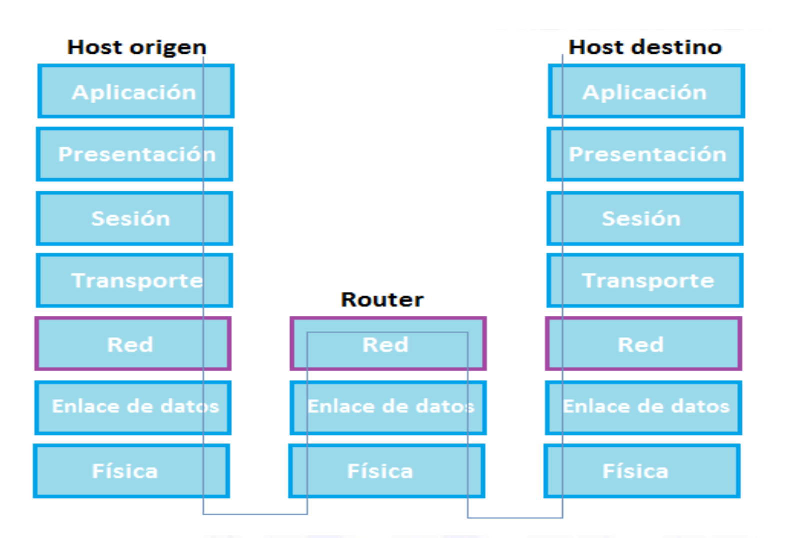


Imagen 5.1 (Modelo de capas – router)

Desde nuestro enfoque de seguridad, lo que nos interesa es poder determinar la "**criticidad**" de los diferentes routers que posee la red. Para ello, recurriremos a una propuesta sencilla:

a. Router crítico: aquel que sostiene un porcentaje muy alto del tráfico de la red.

   En esta categoría de forma sencilla podemos pensar en tres tipos:

   - **Core** (voz, datos y señalización).
   - **Router Reflector.**
   - **Frontera de Banda Ancha** (Internet).

b. Router de criticidad Media: aquel que sostiene un porcentaje inferior al 20.

   Podemos pensar en (PE, interconexión sedes, Anillos Metro Ethernet).

c. Router de baja criticidad: En general los internos o de acceso (Accesos ADSL, MacroLAN, pequeños clientes o partners (CPEs), zonas de servicio no críticas).

Esta clasificación que puede ser discutible, es sencillamente una idea inicial de cómo podemos diseñar nuestra estrategia de seguridad a nivel de red. Básicamente lo que estamos diciendo es que evaluemos el "**Impacto**" que tiene sobre nuestra infraestructura cada uno de estos dispositivos. Tal cual hemos dicho al principio del capítulo, la misión fundamental de estos elementos es la "Conmutación de paquetes", por lo tanto si un router no está disponible, todos las redes o subredes que están conectadas al mismo no recibirán tráfico de paquetes. A medida que la "jerarquía" del router es mayor, es decir mayor porcentaje de tráfico controla, mayor será la cantidad de información que peligra, a su vez cuanto mayor "responsabilidad" tenga ese router, mayor impacto causará (ejemplo: Router Reflector que veremos más adelante). En definitiva, proponemos como primer medida, evaluar este parámetro que hemos presentado como "criticidad".

Dentro de la categoría de router críticos, de forma práctica podemos considerar.

5.2.1. Routers de Core.

(O routers de Núcleo) → para nosotros SIEMPRE son ¡¡CRÍTICOS!!

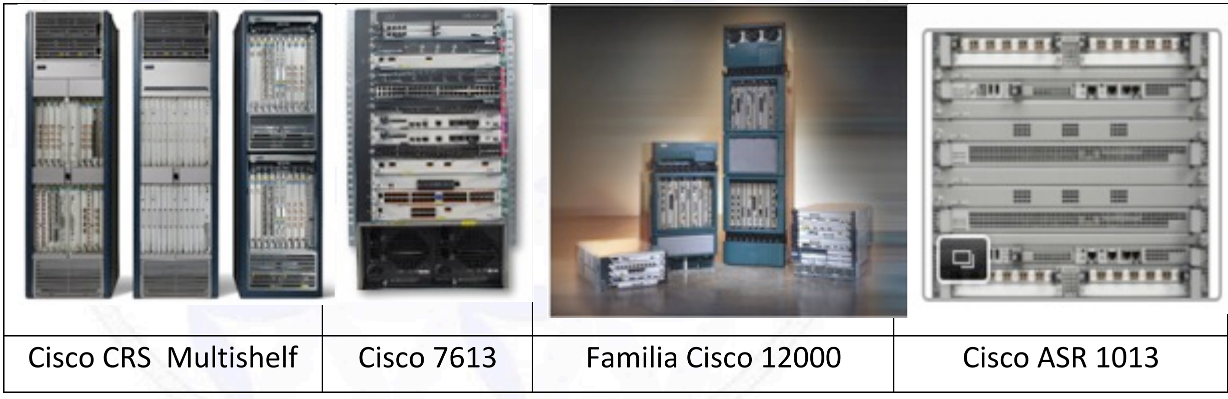
Justamente por ser críticos es que nos detendremos el tiempo suficiente como para comprender lo más que podamos sobre su despliegue y funcionamiento.

> Según Wikipedia: "*En las empresas, el core routers puede proporcionar una columna vertebral interconectando la distribución de los niveles de los encaminadores de múltiples edificios de un campus, o a las grandes empresas locales. Tienden a ser optimizados para ancho de banda alto*".

En las grandes redes, suelen ser routers de alta capacidad, es decir que controlan anchos de banda del orden de varios Gbps, llegando hoy en día a los Tbps.

Hay dos grandes marcas que son líderes de mercado en esta gama (Juniper y Cisco), aunque ahora está entrando de forma muy agresiva Huawei. A título de referencia mencionamos los modelos más frecuentes que encontraremos hoy en grandes redes:

- Familia Cisco: Se puede profundizar en cada uno de ellos en la página Web de Cisco (http://www.cisco.com/c/en/us/products/index.html):
  a) Serie Cisco CRS (Carrier Routing System).
  b) Serie Cisco 7600.
  c) Serie Cisco 12000 XR.
  d) Serie Cisco ASR 1000 y 9000 (ASR: Aggregation Services Routers).
  e) Para redes de menor tamaño están los llamados "Small Business Routers" de las familias 800, 1900 y 2900.
  f) Familia Catalyst (series 6500) y Nexus (serie 7000): En realidad estas dos familias son eminentemente Switchs, pero en la actualidad ofrecen un sinnúmero de posibilidades para configuraciones de niveles superiores.



Cisco CRS Multishelf	Cisco 7613	Familia Cisco 12000	Cisco ASR 1013

Imagen 5.2 (Modelo de router – familia Cisco)

- Familia Juniper: Se puede profundizar en cada uno de ellos en la página Web de Juniper (http://www.juniper.net/us/en/products-services/routing/):
    a) Series Juniper T.
    b) Series Juniper ERX.
    c) Serie Juniper MX.



Juniper T 4000	Juniper ERX 1440	Juniper MX 960

Imagen 5.3 (Modelo de router – familia Juniper)

5.2.2. Router Reflector (RR).

El concepto de router reflector podríamos pensar que nace con el protocolo **BGP** (Border Gateway Protocol) que como hemos mencionado al principio, se trata de un protocolo de enrutamiento dinámico para sistemas autónomos (AS) y en definitiva debe ser el protocolo más importante que comunica las troncales de Internet, de hecho a cada **ISP** (Internet Service Provider), IANA (Internet Authority Numbers Asign) le asigna grandes rangos de direcciones IP agrupados dentro de un as, y este valor será el más importante que se considerará para las rutas que controlan todo Internet. Este protocolo dinámico debe mantener actualizadas las tablas de ruta de estos grandes routers con bastante frecuencia, para poder hacerlo cada uno de ellos necesitaría conocer el estado que posee de las mismas cada uno de sus "vecinos" (*Neighbor*), si no existieran los Router Reflector, esta comunicación debería ser una malla "todos con todos", lo cual evidentemente desgastaría en exceso todo los vínculos de comunicación. Justamente para resolverlo es que todos los router BGP miran o dirigen su mirada (peer) hacia estos RR que son los encargados de recibir los cambios de estas rutas y responder ante cualquier consulta de esta "comunidad de vecinos" o vecindario (neighborhood) a lo que podríamos llamar como "routers clientes" de este RR. Cabe mencionar que el concepto de "peer" también se suele entender como "par",



es decir un router que está conectado a este sistema o que es cliente del mismo, o que es el otro extremo de esta comunicación (*A nivel internacional el tráfico de "peering" son los convenios que firman entre carriers para transportar información de otros carriers a través de sus propios vínculos con condiciones económicas especiales y/o gratuito*).

El concepto de as puede ser dividido en áreas o conjuntos de clientes que se denominan "cluster", donde cada cluster debe tener al menos un RR.

En la actualidad estos RR también se integran o emplean con otras familias de protocolos dinámicos (iBGP y eBGP, IS-IS, OSPF, MPLS) trabajando de la misma forma.

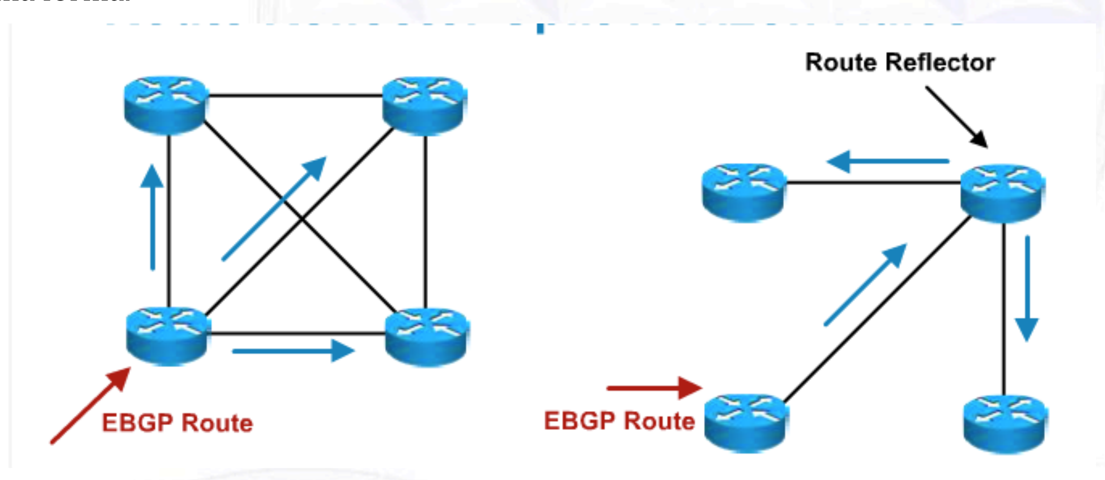


Imagen 5.4 (Router Reflector)

5.2.3. Routers de frontera.

Se trata de cualquier router que posea interfaces conectadas a otro dispositivo que no es de responsabilidad de la propia red, o que finaliza túneles de cualquier tipo con dispositivos también externos a la misma. Un aspecto que también puede considerarse es que el mismo intercambie tráfico hacia estas redes externas a la organización.



Imagen 5.5 (Router de Frontera)

5.2.4. Routers de criticidad media y baja.

En este punto no entraremos en mayores detalles, sólo presentamos como ejemplo el que mayor representa este grupo medio, que es el router **PE** (que ya presentamos al tratar MPLS).

Solo recordemos que en el protocolo MPLS, un router **P** o router Proveedor es un Label Switch Router (LSR) que funciona como un router de tránsito de la red principal, este dispositivos en la práctica se encuentra en una zona "gris" en cuanto a su criticidad, pues dependerá de la jerarquía, ubicación y tipo de tráfico que regule la importancia de su seguridad. Lo que nos interesa, es que estos router **P** típicamente están conectados a uno o más enrutadores de **PE** (Provider Edge). Sobre este último sí que no tenemos duda sobre su impacto, pues en definitiva su disponibilidad sólo afecta a la "zona" que interconecta, sin afectar a los niveles superiores.

Por último reiteremos la idea que estos routers PE, en general son la "puerta de entrada" de los diferentes "clientes" (**CE**: Customes Edge) que hacen unos de la arquitectura propia de red, estos últimos tienen un bajo impacto dentro de nuestra infraestructura, pues son prácticamente el último eslabón de la jerarquía.

5.3. Cómo analizar la configuración y seguridad de un Router.

Esta actividad por ser una de las más importantes de nuestro trabajo de seguridad en redes. En este punto presentaremos la parte teórica y conceptual y a continuación veremos varios ejemplo y ejercicios prácticos.

En una gran red, el trabajo, área o responsable de seguridad en general no es el mismo que el que administra la red, de hecho debería estar claramente separado para no ser "juez y parte". Se evidencia mucho esta separación en grandes redes, cuando la actividad la cumple el mismo área y rutina del día a día va llevando a los responsables de red a crear o modifar, rutas, listas de control de acceso, reglas de firewall, etc.. y la seguridad se va degradando cada vez más.

En nuestra presentación, trataremos este tema como si fuera abordado por una persona responsable de seguridad o auditoría, y que justamente no es quien diseña, planifica y opera la red, por lo tanto su labor es totalmente independiente a la gestión de red, de esta forma nos permitirá hacer un trabajo mucho más detallado. Si no es este el caso del lector, y desempeña varios de estos roles a la vez, es un my buen ejercicio, abordar este tema, intentando enfocarlo desde los diferentes perfiles que se tratarán aquí para poner de manifiesto todas las actividades que no debería dejar de lado, independientemente que su responsabilidad sea sobre todas ellas.

En la práctica el trabajo comienza por comenzar metódicamente a comprender la arquitectura y funcionamiento de la red, realizando lo siguiente:

- Solicitar y recolectar información previa sobre estos dispositivos al área responsable.
- Analizar con todo el detalle posible la arquitectura de la red en cuestión.
- Solicitar una presentación (si se desea) por parte de los responsables de "Planificación" y/o "Ingeniería" de la red.
- Planificar y organizar entrevistas con los administradores de al menos uno de cada uno de los tipos mencionados, o al menos los que consideremos clave en esta revisión de seguridad. Cada una de estas entrevistas deberán ser eminentemente técnicas y con conexión al dispositivo o plataforma que se va a analizar.
- Sentarnos al lado de cada administrador, en su puesto de trabajo o desde el lugar que el prefiera pero con acceso al dispositivo.
- Solicitarle que "loguee" la sesión (para que posteriormente nos entregue toda la actividad realizada, donde como veremos más adelante, figurarán todos los comandos ejecutados y los parámetros de configuración).
- Avanzar con nuestro análisis de su configuración (y "subliminalmente", nuestra evaluación acerca del conocimiento que este administrador "posee" y "comparte" de ese dispositivo).

Conceptualmente los interrogantes que debemos considerar son:

a) ¿Se encuentran adecuadamente documentados los dispositivos?
b) ¿Son correctos los recursos asignados?
c) ¿Se gestionan eficientemente?
d) ¿Cómo está su configuración?
e) ¿Qué mecanismos de control poseen?
f) ¿Qué mecanismos de resguardo y recuperación tienen implementados?

Desarrollemos con más detalle cada uno de ellos:

1) ¿Se encuentran adecuadamente documentados?:

- ¿Existen planos claros y entendibles?
- ¿Representan sus interfaces IP, nombres y zonas que interonectan?
- ¿Se encuentran actualizados?
- ¿Existe algún procedimiento de gestión de routers?
- ¿Se cumple en la realidad?

- Las tareas, usuarios, nombres, contraseñas, etc. ¿Están debidamente documentadas, o las realizan ciertas o una sola persona?

2) ¿Son correctos los recursos asignados?:

- ¿El área está adecuadamente dimensionado?
- ¿El personal dispone del tiempo suficiente?
- ¿Poseen algún tipo de herramientas automatizadas para la gestión de routers?

3) ¿Se gestionan eficientemente?:

- ¿Se emplean los mecanismos de acceso adecuados?
- ¿Emplean protocolos seguros?
- ¿Emplean usuarios genéricos?
- ¿Comparten usuarios y contraseñas?
- ¿Poseen plantillas o parámetros de configuración inicial actualizados?

4) ¿Cómo está su configuración?:

- ¿Es homogénea la configuración de los routers?
- ¿Está actualizada la versión de su sistema operativo?
- ¿Existe un mecanismo de control de acceso por Tacacs o Radius?
- Si existe este mecanismo, ¿Es obligatoria la validación previa por medio de este, y luego en local?
- ¿Emplea contraseñas robustas?
- ¿Existen usuarios genéricos?
- ¿Está adecuada la configuración de envíos de Syslog?, ¿Hacia SIEM?
- ¿Tiene configurada una jerarquía **NTP** (Network Time Protocol)?
- ¿Emplea **SNMP** (Single Network Monitor Protocol?
- ¿Está debidamente configurado el mismo con versión 3?
- ¿Emplea comunidades seguras?
- ¿tiene habilitado snmp para escritura?
- ¿Es coherente esta jerarquía?
- ¿Obliga a emplear **SSH** (Secure SHell) y **sftp** (Secure File Transfer Protocol)?
- ¿Tiene inhabilitadas las interfaces sin usar?

- ¿Aplica **ACLs** (Access Control List) sobre sus interfaces?
- Si es Cisco, ¿Tiene activo el protocolo **CDP** (Cisco Discovery Protocol)?
- En los protocolos dinámicos (Ej: BGP, OSPF), ¿Emplea autenticación de vecinos?
- ¿Posee configurado el Banner previo a su conexión?
- ¿Posee configurado el Banner una vez conectado?

5) ¿Qué mecanismos de control poseen?:

- ¿Se posee una plantilla estándar de parámetros de obligado cumplimiento?, ¿Se verifica periódicamente la misma?
- ¿Existe algún mecanismo de validación de cambios?
- ¿Posee mecanismos de monitorización, supervisión y/o alarmas?
- ¿Se analizan sus Logs?

6) ¿Qué mecanismos de resguardo y recuperación tienen implementados?:

- ¿Cómo hacen los backups?
- ¿Están accesibles y actualizados?
- ¿Se conoce el procedimiento?
- ¿Se hacen pruebas de recuperación?
- ¿Se mantiene un nivel de seguridad sobre los mismos?

Como norma general en la revisión de seguridad de cualquier tipo de redes (y sus dispositivos), nuestro trabajo, podríamos resumirlo de forma práctica en los siguientes pasos:

1) Recolección y análisis previo de su documentación (planos, arquitecturas, nodos, dispositivos, fabricantes, responsables, funciones, obligaciones, etc.
2) Entrevista con responsables del área de "Planificación/ingeniería" y "Operación/gestión/administración / mantenimiento".
3) Sentarnos en un puesto de trabajo de uno, dos o tres administradores de sus nodos principales, para centrar la atención en lo siguiente:
   - ¿Conoce al detalle la infraestructura/plataforma/red?
   - ¿Posee a mano o tiene acceso a los mapas/planos?
   - Se encuentra claramente documentado su trabajo o actividad...... Este tema es fundamental para evitar la "**Imprescindibilidad**": No puede existir PERSONAL IMPRESCINDIBLE en estas tareas. Nuestra experiencia al respecto es que esta es una problemática muy frecuente, deberíamos hacer un esfuerzo en minimizarlo y erradicarlo lo antes posible, pues es un foco de problemas GRAVE.

     Todo esto se soluciona, cuando su tarea se comparte con otros, se documenta al detalle, y se trabaja de forma transparente (*y no egoísta*) dentro del equipo de trabajo. Insistimos en poner como centro de atención este tema y lo penalicemos rigurosamente cuando no se esté cumpliendo.

     NOTA: Antes de su conexión al, o los dispositivos, deberíamos pedirle que "**Loguee**" esta sesión para que luego nos la pueda pasar para analizarla a posteriori. De no ser posible, le pediríamos que luego nos pase los archivos de configuración de ese elemento.
   - ¿Cómo es su metodología de conexión?, ¿Qué protocolos emplea?, ¿Responde a lo que está documentado, o tiene sus propios mecanismos / rutas / herramientas?.
   - ¿Con qué usuario se conecta?, ¿Local, corporativo, el de un Tacacs o Radius, LDAP, etc?
   - ¿Conoce las configuraciones, comandos, significado de los mismos?
   - ¿Se desenvuelve con soltura una vez conectado al dispositivo?
   - ¿Conoce cómo hacer una copia de respaldo y dónde hacerla?
   - ¿Qué haría si debiera recuperar un dispositivo?
   - ¿Es consciente de las medidas de seguridad que deben aplicarse a ese dispositivo?, ¿recibió formación en seguridad?
   - ¿Cuál es el flujo que sigue en la práctica para cualquier tipo de modificación en las configuraciones?, ¿tiene registros de ello?
   - ¿Guarda archivos de configuración o Logs en su ordenador local, o en otros dispositivos? (en particular que no estén documentados).
   - ¿Cómo procede en la práctica ante cualquier tipo de incidencia?
   - ¿Cómo es su administración de Logs?, ¿los conoce?, ¿los controla o mira frecuentemente?, ¿los envía hacia algún otro sitio?
4) A posteriori de la entrevista, deberíamos analizar los archivos de configuración que nos han entregado verificando el nivel de seguridad de los mismos. Esta actividad es la que iremos desarrollando a continuación y con más detalle para cada tipo en particular.

5.4. Aspectos básicos de configuración de seguridad de un Router

Al igual que indicamos para los switchs, en este caso nuevamente la mejor referencia la tendremos en las "**Guías CIS**" que publica el "**Center for Internet Security**" (https://www.cisecurity.org).

En general las configuraciones de un router se realizan por medio de ficheros de texto plano. Si bien existen un sinnúmero de soluciones gráficas para optimizar este actividad, como así también para la gestión, supervisión y monitorización de este tipo de dispositivos, en definitiva, todas ellas terminan operando finalmente sobre este fichero de texto. Cada fabricante tiene sus propias "reglas" de configuración, pero lo importante de esto es que una vez conocida esta metodología, la misma es "unívoca". ¿Qué es lo que queremos transmitir con esto?, pues que toda configuración de un mismo fabricante responde a un esquema básico de parámetros que se deberán escribir en forma y fondo exactamente igual, independientemente del modelo (*es cierto que pueden existir pequeñas diferencias basadas en el número de versión del sistema operativo del router, pero esto no impacta en lo que presentaremos a continuación*).

Cualquier responsable de seguridad de una red que deba evaluar el nivel de bastionado de un router, no debe realizar tareas de "Hacking ético" de caja negra, pues no tiene que demostrar nada, lo que debe hacer es analizar justamente los parámetros que tiene en su configuración cada router de su empresa, por lo tanto su actividad es comprender y analizar configuraciones. Esta actividad no debe ser puntual, pues como bien sabemos, la seguridad se degrada con el tiempo, por lo tanto la mejor forma de realizar este tipo de análisis es de forma periódica y de acuerdo a un "Plan de revisión de seguridad" o "Plan de auditoría". La forma de llevar a cabo este plan, es reuniéndose con las configuraciones, evaluarlas y compararlas con su análisis anterior, es decir trabajar como un ciclo continuo de mejora.

Para realizar este trabajo lo primero es comprender las configuraciones y luego poder realizar las evaluaciones de la forma más eficiente que esté a nuestro alcance.

Manteniendo nuestra línea orientada hacia el software libre, a continuación vamos a trabajar con una herramienta que para los routers Cisco es de gran utilidad "**ccsat**". En nuestro trabajo cotidiano, hemos desarrollado varios scripts que empleamos también para otros vendors como son "Juniper", "Alcatel Lucent (Hoy Nokia)" y "Huawei" basadas en la misma lógica que propone **ccsat**, por esa razón es que nos pareció importante presentar la lógica que esta herramienta emplea pues, comprendiendo esta base, nos resultará extremadamente fácil aplicarla para el análisis de cualquier tipo de dispositivo.

La herramienta "**ccsat**" puede descargarse en: http://ccsat.sourceforge.net

Lo que intentaremos presentar a continuación es una metodología de trabajo que puede ser comprendida a través de la herramienta "ccsat" pero que luego nos permita desarrollar y emplear sencillos "sripts" realizados en programación "bash" para evaluar el nivel de bastionado de cualquier configuración de router.

Una vez descargada “ccsat”, podemos abrirla con cualquier editor de texto.

Lo primero que nos presenta es:

```
#!/bin/sh -

##################################################################
# CCSAT                                 Version 2.2                   #
# Copyright (C) 2003-10 BGK Bill Zeng bgk@hotunix.com               #
#                                       alphan3@yahoo.com             #
# Created: May 9, 2003                  Last Modified: Jan 10, 2010   #
# Script Available at:                  http://ccsat.sourceforge.net  #
#                                       http://hotunix.com/tools      #
###################################################################
# COPYRIGHT NOTICE                                                    #
# Copyright (C) 2003-10  BGK   All Rights Reserved                    #
#                                                                   ʃ #
# CCSAT (Cisco Configuration Security Auditing Tool) is a script to  #
# allow automated audit of configuration security of large numbers   #
# of Cisco routers and switches.  The tool is based upon industry    #
# best practices including Cisco, NSA and SANS security guides and   #
# recommendations.  CCSAT is flexible and can report details down to #
# individual device interfaces, lines, ACL's, as's, etc.             #
#                                                                     #
# Special thanks go to T. Dafoe and J. Reid for sharing knowledge    #
# and resources with the author.  CCSAT has been used on FreeBSD for #
# real audits (20 seconds of runtime for 75 device configurations of #
# 620KB on HP Proliant DL380 with 2.8GHz CPU and 1GB RAM).  It was   #
# also tested on Linux and Solaris-8, and should run on all major    #
# UNIX platforms (POSIX.2-compliant).                                #
#                                                                     #
# CCSAT is freeware, and may be used, modified or redistributed so   #
# long as this copyright & credits notice and the header remain      #
# intact, and be included in documentation.  You agree to indemnify  #
# the author from any liability that might arise from using the code. #
###################################################################
```

Como podemos ver se trata de una herramienta desarrollada en “bash” (`#!/bin/sh`) que es “*freeware*” y “*puede ser utilizada, modificada y redistribuida siempre y cuando los derechos de autor, créditos y cabecera se mantengan intactos, y se incluyan en la documentación*”. Tal cual estamos haciendo en este libro.

No desarrollaremos todo el script, sino solamente las secciones que nos permitan comprender cómo debemos trabajar con este tipo de programas, o cómo podemos desarrollar este tipo de herramientas para que la tarea de evaluación de seguridad de los routers pueda llevarse a cabo como un verdadero ciclo de vida, automatizando todo lo que podamos.

Lo que sigue en el programa es:

```
# Define Variables
```

```
### working, configuration, and reporting directories

workdir=`pwd`
configdir=$workdir/config
reportdir=$workdir/report

### report file, open interface file and temporary files

report=$reportdir/audit-results
fopenif=$reportdir/interfaces_open
f1=$reportdir/tmp1
f2=$reportdir/tmp2
```

Las anteriores, se tratan de una serie de líneas en las cuáles nos quisimos detener pues revistan cierta importancia a la hora de comenzar este tipo de tareas.

Este programa necesita que "subamos" todas las configuraciones que vayamos a analizar a un directorio (`configdir=$workdir/config`) para que, luego de realizarse el análisis, nos entregue un reporte en orto directorio (`reportdir=$workdir/report`). Esta separación de tareas es importante pues si el día de mañana, logramos desarrollar un programa eficiente que trabaje programado (cron) subiendo de forma automática (vís ftp, tftp o sftp) las configuraciones de los routers, se las analice y luego se generen reportes, un buen punto de partida es "separar" los directorios sobre los que se operará. Aquí en realidad lo que está haciendo es, primero posicionarse en el directorio donde como usuarios estamos situados (`` workdir=`pwd` ``) y luego definir dos variables temporales, cada una dentro de los dos directorios (que la herramienta nos especifica que ya deben estar creados (`configdir=$workdir/config` y `reportdir=$workdir/report`). Más abajo declara algunas variables más y dos ficheros temporales.

A continuación nos describe cómo funciona el programa. Solo lo presentamos, pero no nos detendremos en ello.

```
echo "
HOW-TO:

1) To start, have this script (ccsat) in your working directory $workdir;
2) Within that directory, create subdirectories $configdir and $reportdir;
3) Put config text files in $configdir and ensure same file extension
   (default .txt);
4) If none, then add file extension (commands provided here);
5) Run './ccsat 12.4' (assuming 12.4 is the latest IOS);
6) The main report will be $report.
```

Siguen varias decenas de líneas de seguridad en caso de cualquier tipo de fallos (nombres erróneos, directorios no creados, error de extensión de nombre de fichero, etc..), un resumen de parámetros de la totalidad de los routers auditados y la preparación y presentación de los encabezados. No nos detendremos en estas líneas para avanzar directamente sobre los parámetros de configuración.

Antes de pasar a los parámetros concretos sobre los que podemos trabajar, hagamos un alto para hacer un repaso que nos será de máxima utilidad:

Qué es la programación en Bash

Bash es la abreviatura de Bourne again Shell (*Otro Shell Bourne*), se trata de un intérprete de comandos basado en la shell de Linux, su nombre indica que la base es el Shell de **Bourne** (*cuyo nombre viene por su creador* ***Stephen Bourne***) que fue tal vez el primer y más importante interprete de las primeras versiones de Linux a finales de los 70' (pero más limitado que el actual). Bash fue escrito por **Brian Fox** a finales de los 80' y **Chet Ramey** fue su principal sucesor. Es el intérprete por defecto del mayoría de las distribuciones GNU/Linux. Cabe mencionar que hay otros intérpretes como Korn Shell (**ksh**) y el C Shell (**csh**). Durante este texto intentaremos emplear las sintaxis que son comunes a los tres.

A continuación vamos a desarrollar los comandos principales que emplearemos en nuestra labor de auditoría de configuraciones de routers, con estos tendremos la mayor parte del trabajo realizado, pero por supuesto, bash posee muchos más que pueden ser reemplazados, o ampliados por parte del lector para ajustar y desarrollar sus propios scripts.

a. awk

La función básica de awk es buscar líneas en ficheros (u otras unidades de texto) que contienen ciertos patrones. Cuando en una línea se encuentra un patrón, awk realiza las acciones especificadas para dicho patrón sobre esa línea. awk sigue realizando el procesamiento de las líneas de entrada hasta que se llega al final del fichero.

La sintaxis es muy semejante a la del lenguaje C, con la particularidad de que, al ser awk un intérprete, no es necesario pasar por procesos de compilación. awk solo procesa archivos de texto. Para manejar los datos de un documento Word, PDF o de cualquier otro tipo de fichero en formato propietario es necesario exportar la información previamente a algún formato de texto.

Un programa awk consiste en una secuencia de sentencias **acción-patrón**.

Patrón { acción}

La acción se debe separar entre llaves para separarlas de los patrones.

Durante gran parte de esta sección trabajaremos con los archivos reales que nos permitirán entender el funcionamiento del comando.

A continuación presentamos un fichero de configuración real de un router que está en producción, que presenta varios aspectos de mejora y que tomaremos como ejemplo para todo este trabajo.

```
2960_ace#show run

Building configuration...
Current configuration : 858 bytes
!
! Last configuration change at 16:12:07 America Wed Jun 17 2016 by ace
! NVRAM config last updated at 16:12:08 America Wed Jun 17 2016 by ace
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
no service password-encryption
!
hostname 2960_ace
!
logging buffered 163846
no logging console
no logging monitor
enable secret 5 $120h/S3d//2w*wQ08NrFk9O
!
username ace secret 5 $1$cdasW34/8&Vb98/$eR5
aaa new-model
!
aaa authentication login default  group tacacs+ enable
aaa authorization config-commands
aaa authorization exec default  group tacacs+ local
aaa authorization commands 5 default group tacacs+
aaa authorization commands 12 default group tacacs+
aaa authorization commands 15 default group tacacs+
!
!
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh authentication-retries 2
!
interface FastEthernet0/1
 description PISO-1
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/2
 description PISO-2
 switchport access vlan 200
```

```
 switchport mode access
¡
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan100
 ip address 10.1.1.1 255.255.0.0
 no ip route-cache
!
interface Vlan200
 ip address 10.1.2.1 255.255.0.0
 no ip route-cache
!
ip default-gateway 10.1.1.252
no ip http server
no ip http secure-server
logging trap debugging
logging facility syslog
logging source-interface Vlan49
logging 10.1.2.10
logging 10.1.2.12
access-list 2 permit 10.1.2.24
access-list 2 permit 10.1.2.21
snmp-server community private RW
snmp-server community public RO
snmp-server community prueba RW 2
snmp-server trap-source Vlan200
snmp-server packetsize 1024
snmp-server location sede_central
snmp-server enable traps tty
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps power-ethernet police
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 10.1.2.21 version 3
snmp-server host 10.1.2.24 version 3
tacacs-server host 10.1.2.34 key 123456789
tacacs-server host 10.1.2.35 key 123456789
tacacs-server directed-request
!
control-plane
!
```

```
banner motd ^C########################################
#   AVISO: para acceder a este sistema
#   necesita la autorización correspondiente
#   El acceso no autorizado o el uso indebido
#   esta prohibido y es contrario a la
#   legislacion vigente. Toda actividad
#   sobre este sistema sera monitorizada.
####################################
^C
!
line con 0
 password qwerty
line vty 0 4
 session-timeout 5
 privilege level 15
 authorization commands 5 default
 authorization commands 12 default
 authorization commands 15 default
 login authentication default
 transport input ssh
line vty 5 15
!
ntp clock-period 36029500
ntp server 10.1.2.46
end
2960_ace#
```

Para trabajar con esta configuración, lo mejor es copiarla en cualquier directorio empleando Linux, de ser posible bajo el nombre "***2960_ace.txt***" (pues será el que usemos en los ejemplos), posicionarse en ese directorio y desde allí ir realizando las prácticas propuestas.

Ahora sí volvamos a awk.

Vamos a probar este primer ejemplo

```
sh-3.2# awk '/username/ { print $0}' 2960_ace.txt
                username ace secret 5 $1$cdad434/8&Vb98/$eR5
```

Como podemos apreciar en la línea de comandos anterior, llamamos a "awk", a continuación buscamos "/username/" (que es nuestro "**patrón**", pues las barras "/ /" nos encierran el patrón de búsqueda) y luego entre llaves "{ }˝ le decimos que nos imprima (print), en este caso la línea completa que incluye el patrón /username/ (*a continuación veremos otras opciones de impresión*). Vemos también que toda la expresión está encerrada en " ’comillas simples’ (rectas)" (*tecla a la derecha del cero… no confundirlas con las comillas simples inclinadas ``, tecla a la derecha de la "p" que tienen orto significado*), el empleo de estas comillas simples se debe a que el intérprete de comandos (shell) interpretaría esta secuencia como caracteres especiales de la Shell y no como una secuencia "patrón – acción" de awk (*en palabras sencillas: para nosotros su uso será obligatorio!!!*) .

Cabe remarcar que la salida por defecto de "**awk**" es la salida estándar de Linux (*consola*).

En una regla de awk, se puede omitir el patrón o la acción, pero no ambas. El resultado de estas omisiones es el que se presenta a continuación:

```
sh-3.2# awk '/username/' 2960_ace.txt
            username ace secret 5 $1$cdad434/8&Vb98/$eR5
```

o por el contrario:

```
sh-3.2# awk '{ print $0}' 2960_ace.txt
            username ace secret 5 $1$cdad434/8&Vb98/$eR5
        2960_ace#
        Building configuration...
        Current configuration : 858 bytes
        !
        ! Last configuration change at 16:12:07 America Wed Jun 17 2016 by ace
        ! NVRAM config last updated at 16:12:08 America Wed Jun 17 2016 by ace
             !
```

………………… todas las líneas de este fichero (es decir la configuración completa de este router.

Para ser prácticos en nuestros ejemplos, vamos a definir "registro" como cada línea de texto del archivo de entrada que estemos analizando, awk leerá la entrada línea a línea, cada una de ellas finalizará con un salto de línea que en Unix es el caracter **"/n"** (*new line*), al encontrar este valor, awk da por finalizado ese registro, entonces cada registro tendrá "n" cantidad de campos (*o palabras*). Cada campo puede ser referenciado por su posición: $1, $2, $3…….hasta el último que se representa con **$NF**. Otro campo a destacar el campo **$0** que representa todo el registro (*la línea completa*).

La situación más habitual es aquella en la cual cada registro contiene una frase y los campos son las palabras de la frase. El carácter delimitador es el espacio que separa cada palabra de la siguiente, este separador puede modificarse por cualquier otro mediante el parámetro "**–F**" (*con mayúscula*), con él se puede indicar a awk qué carácter debe considerar como separador de campos si se deseara emplear otro.

Para continuar con más ejercicios, nos situaremos nuevamente en la carpeta donde hemos subido nuestra configuración de ejemplo.

Volvamos a analizar nuestro ejemplo anterior:

```
sh-3.2# awk '/username/ { print $0}' 2960_ace.txt
            username ace secret 5 $1$cdad434/8&Vb98/$eR5
```

En el ejemplo anterior, cuando awk encuentra líneas que contengan 'username', éstas son impresas al completo, ya que '**print $0**' hace que se imprima toda la línea

actual. Recordemos el empleo de las "/" alrededor de "username" que nos indicaban cuál es el patrón de búsqueda, en nuestro caso es justamente "username". Este tipo de patrón se llama expresión regular.

En el ejemplo anterior lo hemos hecho únicamente sobre el fichero *2960_ace.txt* Podríamos hacerlo sobre la totalidad de los ficheros. Para poder seguir mejor esta guía cada lector con sus propias configuraciones, invitamos a que descarguen de Internet o desde sus propias redes otros ficheros de configuración "show running config", por ahora solamente de routers de marca Cisco y los guarden en este mismo directorio de trabajo (*Supongamos que hemos subido más routers a nuestro directorio para continuar con estos ejemplos, en este texto lo haremos con dos routers más*):

```
sh-3.2# awk '/username/ { print $0}' *
      username ace secret 5 $1$cdad434/8&Vb98/$eR5
      username red_y_TI secret 5 $1$nC4r9$$rHFg6hjmrG40
      username backup password 7 12090404011C03162E
      username prueba password 7 0822455D0A16
      username juan privilege 15 secret 5 $1$.as23.$_81jS4w
      username cisco privilege 15 secret 5 $1$oPd29Vc3Y9NL1
```

Otro ejemplo más (Llamémoslo "entubar" o "concatenar" comandos). Esta acción se realiza en Linux, empleando el operador "**pipe**" "**|**" ([ALT] + 1). El intérprete de comandos irá ejecutando los comandos concatenados (pipe) siempre de izquierda a derecha. Veámoslo con un ejemplo:

```
sh-3.2# ls -l
      total 152
      -rwxrwxrwx@ 1 ace  staff   9461 20 ene 11:56 2960_ace.txt
      -rwxrwxrwx@ 1 ace  staff  47001 15 dic 18:21 7200_ace.txt
      -rw-r--r--@ 1 ace  staff  15704 14 ene 14:33 CRS_ace.txt
```

Vemos la información detallada de los archivos que contiene el directorio en el que estamos situados (*en nuestro ejemplo en mi directorio, en estos momentos tengo subidos tres routers: 2960_ace.txt, 7200_ace.txt y CRS_ace.txt*), cada campo está separado por un espacio. Por ejemplo, aprovechemos "awk" para seleccionar los archivos del mes de "ene", concatenando ambos comandos:

```
sh-3.2#  ls -l | awk '/ene/ {print $0}'
      -rwxrwxrwx@ 1 ace  staff   9461 20 ene 11:56 2960_ace.txt
      -rw-r--r--@ 1 ace  staff  15704 14 ene 14:33 CRS_ace.txt
```

Aprovechando esta consulta volvamos al separador de campos (opción: "**-F**"):

```
sh-3.2#  ls -l | awk -F':'  '{print $0}'
      total 152
      -rwxrwxrwx@ 1 ace  staff   9461 20 ene 11:56 2960_ace.txt
```

```
-rwxrwxrwx@ 1 ace  staff  47001 15 dic 18:21 7200_ace.txt
-rw-r--r--@ 1 ace  staff  15704 14 ene 14:33 CRS_ace.txt
```

Analizando la respuesta anterior *parecería* que es la misma que lo ejecutado anteriormente, esto se debe a que hemos puesto como acción el valor del campo completo "**$0**", pero si ahora analizamos cada campo veremos que con la opción " **–F**':' " ahora los campos son diferentes:

```
sh-3.2#  ls -l | awk -F':'  '{print $1}'
      total 152
      -rwxrwxrwx@ 1 ace  staff   9461 20 ene 11
      -rwxrwxrwx@ 1 ace  staff  47001 15 dic 18
      -rw-r--r--@ 1 ace  staff  15704 14 ene 14

sh-3.2#  ls -l | awk -F':'  '{print $2}'
      56 2960_ace.txt
      21 7200_ace.txt
      33 CRS_ace.txt

sh-3.2#  ls -l | awk -F':'  '{print $3}'
      ………….. no hay campos……
```

En el primer ejemplo, encadenamos por medio de "|" (pipe) el comando "ls" y le dijimos a awk que busque en la séptima posición ($7) si es igual a "ene". Luego continuamos realizando pruebas con los diferentes campos que nos ofrece esta concatenación.

Como acabamos de ver, cuando awk lee un registro de entrada, el registro es automáticamente separado o particionado por el intérprete en partes, llamadas campos. Para referirse a un campo en un programa, awk usa un signo de dólar **'$'**, seguido por el número de campo que se desee. Por lo tanto, $1 se refiere al primer campo, $2 se refiere al segundo, y así sucesivamente.

Por ejemplo vamos a crear un fichero de texto en nuestro directorio de trabajo que llamaremos "*`ejemplo.txt`*" con el siguiente contenido:

```
La actividad de seguridad en red es fascinante.
```

Si ejecutamos **awk** sobre este ficheros, veremos:

```
sh-3.2# awk ' { print $0 }' ejemplo1.txt
      La actividad de seguridad en red es fascinante.
```

Probemos diferentes opciones de print:

```
sh-3.2# awk ' { print $1 }' ejemplo1.txt
      La
```

```
sh-3.2# awk ' { print $2 }' ejemplo1.txt
      actividad

sh-3.2# awk ' { print $3 }' ejemplo1.txt
      de

sh-3.2# awk ' { print $NF }' ejemplo1.txt
      fascinante.

sh-3.2# awk ' { print $1, $NF }' ejemplo1.txt
      La fascinante.
```

Aquí el primer campo **$1** es "*La*", el segundo o **$2** es "*actividad*" y así sucesivamente, teniendo en cuenta que en esta frase, el último campo o **$8** es "*fascinante*." ya que no hay espacios entre la "e" y el ".", el punto se considera parte de ese campo. Si en nuestro ejemplo buscáramos el campo **$9**, el resultado sería una cadena vacía pues este no existe.

No importa cuántos campos existan, el último campo de un registro puede ser representado por **$NF**, por lo que en ejemplo anterior $ sería lo mismo que $NF.

Volvamos a nuestros primeros ejemplos, nuevamente en la carpeta en la que tengo todos lso routers:

```
sh-3.2# awk '/username/ { print $1, $NF}' *
      username $1$cdad434/8&Vb98/$eR5
      username $1$nC4r9$$rHFg6hjmrG40
      username 12090404011C03162E
      username 0822455D0A16
      username $1$.as23.$_81jS4w
      username $1$oPd29Vc3Y9NL1
```

Busquemos por ejemplo el empleo de password 7:

```
sh-3.2# awk '/password 7/ { print $1, $NF}' *
      username 12090404011C03162E
      username 0822455D0A16
```

Hagamos un alto en este punto.

La metodología de configuración de contraseñas en los routers ofrece diferentes posibilidades y cada fabricante presenta su metodología particular, en todos ellos existen mayores o menores niveles de seguridad que podemos considerar. En los comandos que estábamos presentando por ejemplo, acabamos de ver dos casos típicos dentro de los routers Cisco:

```
      username red_y_TI secret 5 $1$nC4r9$$rHFg6hjmrG40
```

username backup ***password 7*** *12090404011C03162E*

La primera de ellas responde al algoritmo MD5 con un importante nivel de seguridad (*por supuesto siempre y cuando empleemos una política de contraseñas robustas y no empleemos contraseñas triviales, ni predecibles*) y el segundo caso "password 7" es el típico mal uso de contraseñas y está remarcado en todas las buenas prácticas de seguridad como "NO USAR", se trata de un algoritmo totalmente trivial propiedad de este fabricante.

Acabamos de ver cómo a través de un sencillo uso del comando "**awk**" podemos evaluar todas las configuraciones de los routers que deseemos. En este caso por ejemplo, buscando si se está empleando o no "**password 7**" (*awk '/password 7/ { print $1, $NF}' **). Ejecutando esta sencilla línea dentro del directorio donde tengamos los ficheros de configuración (*o por ejemplo los backups*) de todos los routers de la organización, como acabamos de ver, nos presentará todo el listado de usuarios que tienen configurado esta mala práctica.

Volvamos a nuestro punto de partida de esta sección y analicemos qué hace "**ccsat**" para evaluar "password 7". Si buscamos dentro de este script, encontraremos las siguientes líneas:

```
## SRCH="enable password 7 "
SRCH="enable password"
echo "enable password..."
echo "'enable password' (weak) still configured on..." >> $report
numcfged=`grep "$SRCH" * | wc -l | awk '{print $1}'`
echo $numcfged of $numfiles devices >> $report
if (test "$numcfged" != "0" -a "$numcfged" != "$numfiles") then
    grep -l "$SRCH" * >>$report
fi
echo "" >> $report
```

Esta sección del script, primero define una variable (*SRCH="enable password"*), la presenta en pantalla o salida estándar (*echo "enable password..."*).

La redirige hacia un fichero (*) (*echo "'enable password' (weak) still configured on..." >> $report)*

Luego sí hace el trabajo de búsqueda. (*numcfged=`grep "$SRCH" * | wc -l | awk '{print $1}'`)*

Analicemos en detalle este línea paso a paso:

- - define una variable "***numcfged=***"
- realiza un grep: "***grep "$SRCH" **** " (si hiciéramos sólo este grep, la salida sería: *7200_ace.txt: enable password 7 12090404011C03162E*
  CRS_ace.txt: enable password 7 0822455D0A16

Es decir, los dos routers que tienen configurada password 7

- Esta salida del “grep” la concatena con “ | wc -l”, por lo tanto como tiene dos líneas, el comando wc (word count) me entrega como resultado un “2”
- La´última parte de esta concatenación (awk '{print $1}') es solamente para quedarse con el primer valor de esta respuesta (en nuestro caso el “2”)

Por último, se realiza un “test” y un “if” (que probablemante podría optimizarse) para comparar la cantidad de ficheros que existen, respecto a los que tienen configurado “enable passowrd”: *if (test "$numcfged" != "0" -a "$numcfged" != "$numfiles") then grep -l "$SRCH" * >>$report fi*)

(*) Remarquemos un detalle que tal vez se nos pase por alto pero desde el punto de vista del concepto de “redirección” en Linux en muy importante. En la línea que estamos comentando, se ve que la redirección es hacia “**>> $report**”. Una “redirección” en Linux sólo puede hacerse hacia un fichero, y en este caso vemos que se trata de una variable (*por el “$”*). Para aclarar esto, necesitamos volver a las líneas iniciales del fichero “ccsat” que presentamos al inicio y en ellas prestar atención a: “report=$reportdir/audit-results”, como podemos apreciar aquí, esta variable “report” está definida como un fichero que se aloja en el directorio que hemos creado para “reportes”.

Como acabamos de ver, esta sección del programa “**ccsat**” solo nos ofrece información numérica del empleo de password 7. El objetivo de todo esto que estamos desarrollando es justamente poder avanzar técnicamente en la seguridad de nuestras redes, para ello es que proponemos comprender estos sencillos comandos bash, también los diferentes desarrollos de open source del mercado (como en este caso estamos viendo con ccsat) y a través de ello, desarrollar y ejecutar nuestros propios programas para mejorar el trabajo en nuestras organizaciones. En este caso por ejemplo nos interesaría poder incrementar la información que nos ofrece “ccsat” incorporando también a nuestro análisis el listado de las password 7 que están configurados en nuestras redes.

Ya hemos visto que podemos ejecutar:

```
sh-3.2# awk '/password 7/ { print $1, $NF}' *
        username 12090404011C03162E
        username 0822455D0A16
```

Lo mismo podríams realizar con:

```
sh-3.2# awk '/password 7/ { print $0}' *
        enable pasword 7 12090404011C03162E
        enable pasword 7 0822455D0A16
```

Si quisiéramos también tener el nombre de los ficheros de configuración de los routers que tienen esta configuración podríamos hacerlo con:

```
sh-3.2# grep "$SRCH" *
    7200_ace.txt: enable password 7 12090404011C03162E
    CRS_ace.txt: enable password 7 0822455D0A16
```

Es decir, tenemos varias formas de poder seguir avanzando, en la medida que conozcamos cómo realizar las consultas de forma adecuada.

En nuestro trabajo ya hemos podido identificar una mala práctica por parte de los administradores de estos dispositivos, un paso más podría ser decriptografiar estas contraseñas para seguir avanzando en nuestra evaluación o directamente para informar a las áreas correspondientes con las evidencias adecuadas, que así como nosotros lo hemos hecho, también lo puede hacer cualquier intruso. Para esta actividad presentamos a continuación otro sencillo script, esta vez desarrollado en "perl" que se denomina: "**ciscocrack.pl**" (en Internet, existen muchos más programas para esta tarea).

```
#
#!/usr/bin/perl -w
# $Id: cisco.passwords.html 3722 2006-07-28 03:53:26Z fyodor $
#
# Credits for orginal code and description hobbit@avian.org,
# SPHiXe, .mudge et al. and for John Bashinski
# for Cisco IOS password encryption facts.
#
# Use for any malice or illegal purposes strictly prohibited!
#
#
# Usage: perl cisco_passwd_decrypt.pl some_encrypted_password
#

@xlat = ( 0x64, 0x73, 0x66, 0x64, 0x3b, 0x6b, 0x66, 0x6f, 0x41,
          0x2c, 0x2e, 0x69, 0x79, 0x65, 0x77, 0x72, 0x6b, 0x6c,
          0x64, 0x4a, 0x4b, 0x44, 0x48, 0x53 , 0x55, 0x42 );

                $dp = "";
                ($s, $e) = ($ARGV[0] =~ /^(..)(.+)/o);
                for ($i = 0; $i < length($e); $i+=2) {
                    $dp .= sprintf "%c",hex(substr($e,$i,2))^$xlat[$s++];
                }
        print "+----------------------------------------------------+\n";
        print "| Decrypting an encrypted password from a Cisco device |\n";
        print "+----------------------------------------------------+\n";
        print "$dp\n";
        print "+----------------------------------------------------+\n";
# eof
```

Si instalamos y ejecutamos este programa sobre las password 7 que encontramos en nuestros routers de ejemplo, el resultado sería el siguiente:

```
sh-3.2# ./ciscocrack.pl 0822455D0A16
    +----------------------------------------------------+
    | Decrypting an encrypted password from a Cisco device |
```

```
    +-----------------------------------------------------+
    cisco
    +-----------------------------------------------------+
sh-3.2# ./ciscocrack.pl 12090404011C03162E
    +-----------------------------------------------------+
    | Decrypting an encrypted password from a Cisco device |
    +-----------------------------------------------------+
    password
    +-----------------------------------------------------+
```

Como pudimos apreciar, las dos contraseñas de nuestros routers de ejemplo son: "*cisco*" y "*password*"

Ahora que ya empezamos a ver los resultados de emplear programación en bash, sigamos adelante con nuestro primer comando "**awk**"

La sentencia **print** realiza la salida con un formato estandarizado y simple. Solo es necesario especificar las cadenas o números que van a ser impresos en una lista separada por comas. Ellos son impresos separados por espacios en blanco, seguidos por un carácter newline o retorno de carro. La sentencia presenta la siguiente forma:

print iteas, item2, ...

Los paréntesis son necesarios si algunos de las expresiones items utiliza un operador relacional. Los operados relacionales son `==', `!=', `<', `>', `>=', `<=', `~' y `!~'

Los items impresos pueden ser cadenas constantes o números, campos del registro actual (tal y como $1), variables, o cualquier expresión awk. La sentencia print es completamente general para procesar cualquier valor a imprimir. Para imprimir una parte de texto fija, se debe utilizar una constante cadena tal y como "La fecha de hoy es:" como item.

Un ejemplo (con salto de línea "**\n**"):

```
sh-3.2# awk 'BEGIN { print "línea uno\nlínea dos\nlínea tres" }'
    línea uno
    línea dos
    línea tres
```

Un pequeño pero significativo detalle es el empleo de comas entre los campos de impresión, por ejemplo:

```
sh-3.2# awk '{ print $1 $2 }' ejemplo1.txt
    Laactividad

sh-3.2# awk '{ print $1, $2 }' ejemplo1.txt
    La actividad
```

Si empleáramos los últimos conceptos, podríamos tener una salida más clara:

```
sh-3.2# awk '{ print "las primeras dos palabras son: "$1, $2 }'
ejemplo1.txt
las primeras dos palabras son: La actividad
```

Ordenadores booleanos.

De las diferentes alternativas que ofrece awk, nos centraremos únicamente en dos: **and (&&)** y **or (||).** Para cualquiera de ellas se puede implementar la negación **(!)** y los presentaremos con los ejemplos que figuran a continuación:

```
sh-3.2# awk '/username/ { print $0}' *
    username ace secret 5 $1$cdad434/8&Vb98/$eR5
    username red_y_TI secret 5 $1$nC4r9$$rHFg6hjmrG40
    username backup password 7 12090404011C03162E
    username prueba password 7 0822455D0A16
    username juan privilege 15 secret 5 $1$.as23.$_81jS4w
    username cisco privilege 15 secret 5 $1$oPd29Vc3Y9NL1

sh-3.2# awk '/password/ { print $0}' *
    username backup password 7 12090404011C03162E
    username prueba password 7 0822455D0A16

sh-3.2# awk '/privilege/ || /password { print $0}' *
    username backup password 7 12090404011C03162E
    username prueba password 7 0822455D0A16
    username juan privilege 15 secret 5 $1$.as23.$_81jS4w
    username cisco privilege 15 secret 5 $1$oPd29Vc3Y9NL1

sh-3.2# awk '/privilege/ || /secret/ { print $0}' *
    username ace secret 5 $1$cdad434/8&Vb98/$eR5
    username red_y_TI secret 5 $1$nC4r9$$rHFg6hjmrG40
    username juan privilege 15 secret 5 $1$.as23.$_81jS4w
    username cisco privilege 15 secret 5 $1$oPd29Vc3Y9NL1

sh-3.2# awk '/privilege/ && /secret/  { print $0}' *
    username juan privilege 15 secret 5 $1$.as23.$_81jS4w
    username cisco privilege 15 secret 5 $1$oPd29Vc3Y9NL1
```

Veamos por último las opciones de negación de este caso:

```
sh-3.2# awk '/privilege/ && ¡/password { print $0}' *
    username juan privilege 15 secret 5 $1$.as23.$_81jS4w
    username cisco privilege 15 secret 5 $1$oPd29Vc3Y9NL1
```

```
sh-3.2# awk '!/privilege/ && /secret/ { print $0}' *
      username ace secret 5 $1$cdad434/8&Vb98/$eR5
      username red_y_TI secret 5 $1$nC4r9$$rHFg6hjmrG40
```

Ejemplos prácticos de uso:

El ejemplo siguiente imprime todas las líneas que tengan más de 80 caracteres de todos los archivos del presente directorio:

```
sh-3.2# awk 'length($0) > 80' *
```

El ejemplo siguiente imprime todas las líneas que tengan al menos un campo. Es una forma fácil de eliminar líneas en blanco.

```
sh-3.2# awk 'NF > 0'
```

El ejemplo siguiente suma todas las ocurrencias de "*username*". El operador para añadir 1 se escribe **'++'**. Puede ser usado para incrementar una variable antes o después de obtener su valor

```
sh-3.2# awk 'BEGIN { print "Análisis de 'username'" } /username/ { ++usernamebar } END { print "'username' aparece " usernamebar " veces." }' *
Análisis de username
username aparece 10 veces.
```

A continuación seguiremos con la presentación más detallada de varios de los comandos que hasta ahora hemos ido tratando.

b. test

Otro comando que se acaba de presentar en el ejemplo anterior es "test".
Su formato es: **test expresión**

Este comando evalúa la expresión, si es correcta retorna cero (true), si no lo es retorna 1 (false).

nos interesa considerar la opción "**-a**", en la cual se evalúan dos expresiones (expresión1 -a expressión2), si AMBAS son verdaderas, entrega un **cero**, si cualquiera de las dos es falsa, será un **uno**.

c. sort

su formato es: **sort [opciones] [archivo]**

sort <u>ordena líneas de archivos de texto</u> y escribe el resultado en la salida estándar (salida estándar por consola, eco por consola). De todo lo que ofrece para nuestro trabajo nos interesan especialmente las siguientes opciones:

"-u" que no repite líneas ordena sólo una ("u":unique) instancia de cada repetición que exista
"-b" que ignora líneas en blanco
"-f" ignora mayúsculas y minúsculas

d. <u>wc</u> (word count)

wc ya lo hemos presentado también en los primeros ejemplos y su formato es:
wc [clmw] [file ...]

wc cuenta y muestra el número de líneas, caracteres, palabras y bytes de cada archivo solicitado y envía su resultado a la salida estándar

"-c" cuenta bytes
"-l" cuenta líneas
"-m" cuenta caracteres
"-w" cuenta palabras

Veamos ejemplos (creemos cualquier fichero de ejemplo, llamémoslo "ejemplo_wc.txt" y trabajemos sobre el mismo), no es necesario que pasemos aquí este formato de ejemplo, solo se presentan los resultados para que el lector pueda analizarlos e intentar reproducir un fichero que entregue las mismas respuestas:

```
sh-3.2# wc -c ejemplo_wc.txt
      50 ejemplo_wc.txt

sh-3.2# wc -l ejemplo_wc.txt
      16 ejemplo_wc.txt

sh-3.2# wc -m ejemplo_wc.txt
      49 ejemplo_wc.txt

sh-3.2# wc -w ejemplo_wc.txt
      15 ejemplo_wc.txt
```

e. <u>grep</u>

grep como hemos visto, busca patrones en cualquier tipo de archivo o directorio (*en muchos casos es similar a lo que hemos visto de awk*). Presentaremos a continuación las opciones que más nos interesan para estas tareas con routers.

"-i" ignora mayúsculas o minúsculas

"-n" inserta el número de línea donde lo encontró
"-l" solo presentará el nombre de los archivos que contienen en alguna línea el patrón buscado

Ejemplos en relación con este trabajo:

```
sh-3.2# grep –l banner *
2960_ace.txt
```

generar quiénes tienen banner:

```
grep -l banner * > tienen
```

generar un listado de todos los routers a analizar:

```
ls  > todos
```

Quedarnos solo con el que NO tiene banner:

```
grep -l "banner" * | awk -F':' '{print $1}' | sort -u >tienen; ls >todos; diff tienen todos | grep -i txt | awk '{print $2}'
```

Empleo de **"^"** en grep

Si colocamos:
grep -l 'authentication' *
buscará línea a línea en todos los ficheros la ocurrencia de la palabra 'authentication'

Si colocamos:

```
grep -l '^authentication' *
```

Buscará línea a línea en todos los ficheros la ocurrencia de la palabra 'authentication' AL PRINCIPIO de cada línea. En nuestro directorio de trabajo sería:

```
sh-3.2# grep -l 'authentication' *
        2960_ace.txt
        7200_ace.txt
        CRS_ace.txt
```

Como pudimos ver, nos presenta los tres routers pues todos ellos tienen configurada alguna línea que hace mención a "autentication", sin embargo si pusiéramos:

```
sh-3.2# grep -l '^authentication' *
……….(ninguna)
```

No nos dará ningún resultado, pues ninguna línea de estas configuraciones comienza con esta palabra.

f. asignación de variables:

El resultado de la ejecución de cualquier comando Linux, pasa primero por la función **"main"** cuya tarea es verificar que el mismo se ejecutó correctamente o no. De forma similar al comando "**test**", la función **main**, entregará un "0" (cero) si el comando funcionó correctamente y cualquier otro valor si el mismo presentó algún error, este valor dependerá de cada comando (*pueden ser varios tipos de valores dependiendo del error dependiendo de cada comando específico*).

Toda esta presentación viene a cuento de que al asignar una variable en linux, dependiendo del formato en que lo redactemos, la misma obtendrá un valor u otro.

por ejemplo:

```
sh-3.2# bb=`grep "username" 2960_ace.txt`
sh-3.2# echo $bb
      username ace secret 5 $1$cdad434/8&Vb98/$eR5

sh-3.2# bb=$( grep "username" 2960_ace.txt )
sh-3.2# echo $bb
      username ace secret 5 $1$cdad434/8&Vb98/$eR5
```

Si bien los dos formatos anteriores entregan el mismo resultado, debemos mencionar que el formato estándar (que soporta: bash, kshell, cshell) es el segundo de ellos **"=$( )",** el primero si bien es muy empleado, sólo lo interpreta bash.

Por último si no empleamos ninguno de ellos, la variable no interpreta el comando:

```
sh-3.2# bb=grep "username" 2960_ace.txt
sh: username: command not found
```

g. diff:

Formato: **diff [opciones…] archivos**
diff compara archivos línea a línea.
- **"-i"** ignora mayúsculas o minúsculas
- **"-b"** ignora diferencias entre los espacios en blanco de un archivo y otro
- **"-w"** ignora todos espacios
- **"-B"** ignora líneas en blanco
- **"-a"** trata todos los archivos como texto
- **"-n"** salida normal

h. tee:

tee "concatena" o copia una entrada estándar hacia cero o más archivos.

"-a" concatena (apenda) sin sobre escribir el fichero indicado

si no se emplea la opción "-a", se sobre escribe todo lo anterior, es decir se crea un fichero nuevo.

Volvamos a aplicar estos conceptos con nuestro ejemplo de configuración.

Otro protocolo importante para considerar en la seguridad de un router es el protocolo **SNMP** (Single Network Monitor Protocol) pues a través del mismo es posible obtener mucha información de la red y a su vez cuando está habilitada la opción de escritura (write) se puede modificar todo tipo de parámetros en los dispositivos haciendo uso de los valores adecuados, este protocolo en su versión 3 que es la única que ofrece seguridad lo hemos desarrollado ya en el libro "**Seguridad por Niveles**". Veamos cómo aplicar los conceptos de bash que acabamos de aprender en el control de la configuración de este protocolo.

Lo primero que evaluaremos es la existencia de "comunidades" por defecto de escritura y lectura, tomando como base nuevamente "ccsat" pero desarrollando nosotros el detalle que estamos buscando.

Una forma puede ser a través de las siguientes líneas en bash (*primero presentamos las líneas que pueden ser incorporadas a ccsat y luego repetimos el script con las explicaciones pertinentes*):

```
SRCH="^snmp-server community "
SRCH2="public"
SRCH3="private"
echo "Auditando comunidades SNMP public/private...
"
echo "   a. Empleo de comunidades por defecto (public/private)" >> $report
echo "" >> $report
echo "Comunidades por defecto configuradas en estos routers:" " >> $report
numcfged1=`grep "$SRCH" * | grep -w "$SRCH2" | wc -l | awk '{print $1}'`
numcfged2=`grep "$SRCH" * | grep -w "$SRCH3" | wc -l | awk '{print $1}'`
echo "Comunidades por defecto: "  $numcfged1 \(ro\) y $numcfged2 \(rw\)
configuradas en los siguientes dispositivos: >> $report
if [ "$numcfged1" != "0" -a "$numcfged1" != "$numarchivos" ] ; then
    grep "$SRCH" * | grep -w "$SRCH2" >> $report
fi
if [ "$numcfged2" != "0" -a "$numcfged2" != "$numarchivos" ] ; then
    grep "$SRCH" * | grep -w "$SRCH3" >> $report
fi
echo "" >> $report
```

```
SRCH="^snmp-server community "  → Definición de variables
SRCH2="public"  → Definición de variables
SRCH3="private"  → Definición de variables
echo "Auditando comunidades SNMP public/private...
"  → eco de mensaje por pantalla
echo "Empleo de comunidades por defecto (public/private)" >> $report  →
redirección del mensaje el fichero de reporte final
```

```
      echo "" >> $report  → se deja un espacio en blanco en el fichero
      echo "Comunidades por defecto configuradas en estos routers:" >>$report
→título
      numcfged1=`grep "$SRCH" * | grep -w "$SRCH2" | wc -l | awk '{print $1}'`
→ Nro. Ficheros que tienen comunidad "public"
      numcfged2=`grep "$SRCH" * | grep -w "$SRCH3" | wc -l | awk '{print $1}'`
→ Nro. Ficheros que tienen comunidad "private"
      echo "Comunidades por defecto: "  $numcfged1 \(ro\) y $numcfged2 \(rw\)
configuradas en los siguientes dispositivos: >> $report   → redirección del los
valores calculados y título al fichero de reporte
if [ "$numcfged1" != "0" -a "$numcfged1" != "$numarchivos" ] ; then
    grep "$SRCH" * | grep -w "$SRCH2" >> $report
fi    → si "public" existe, nos presenta los router donde está (grep…)
if [ "$numcfged2" != "0" -a "$numcfged2" != "$numarchivos" ] ; then
    grep "$SRCH" * | grep -w "$SRCH3" >> $report
fi   → si "private" existe, nos presenta los router donde está (grep…)

echo "" >> $report
```

En nuestra configuración de ejemplo "**2960_ace.txt**" vemos que existen dos líneas que presentan esta mala práctica, ellas son:

snmp-server community private RW
snmp-server community public RO

Es decir, en ellas tenemos ambas comunidades por defecto, y a su vez se está permitiendo la escritura con esta comunidad (private). Supongamos que este es el único dispositivo que tiene este fallo de seguridad, en ese caso la salida de estas líneas de script en el fichero de reporte final (`report=$reportdir/audit-results`) sería:

```
      Analizando SNMP
         .a. Empleo de comunidades por defecto (public/private)

      Comunidades por defecto configuradas en estos routers:
      Comunidades por defecto:  1 (ro) y 1 (rw) configuradas en los siguientes
dispositivos:
      2960_ace.txt: snmp-server community public RO
      2960_ace.txt: snmp-server community private RW
```

Para seguir avanzando en este tipo de evaluaciones, profundicemos más aún en este protocolo y veamos cómo podemos analizar la configuración de la versión 3 del mismo. Manteniendo el mismo esquema de trabajo con bash tomando como base "ccsat" lo que podemos incorporar a este programa puede ser algo como lo que se presenta a continuación (*nuevamente presentamos primero las líneas, y luego las mismas con sus comentarios*).

```
# Buscando si emplean SNMPv3

SRCH="^snmp-server host [0-9*]"
SRCH2="version 3"
echo "Auditando SNMP version 3...
.........
```

```
"
echo "   b. Empleo de SNMP versión 3" >> $report
echo "" >> $report

numcfged=`grep "$SRCH" * | grep "$SRCH2" | awk -F':' '{print $1}' | sort
-u | wc -l | awk '{print $1}'`
echo "SNMP versión 3 NO configurado en" `expr $numarchivos - $numcfged`
de $numarchivos dispositivos >> $report
grep -l "$SRCH2" * | awk -F':' '{print $1}' | sort -u >$f1; ls >$f2;
diff $f1 $f2 | grep -i $cfgfileext | awk '{print $2}' | tee -a $report
rm -rf $f1 $f2
```

A continuación comentamos cada línea.

```
# Buscando si emplean SNMPv3

SRCH="^snmp-server host [0-9*]"  → Definición de variables
SRCH2="version 3"   → Definición de variables
echo "Auditando SNMP version 3...    → eco de mensaje por pantalla
.........
"
echo "   b. Empleo de SNMP versión 3" >> $report      → redirección del
mensaje el fichero de reporte final
echo "" >> $report  → se deja un espacio en blanco en el fichero

numcfged=`grep "$SRCH" * | grep "$SRCH2" | awk -F':' '{print $1}' | sort
-u | wc -l | awk '{print $1}'`  → Nro. Ficheros que tienen, primero un snmp-
server configurado, y luego los que emplean version 3
echo "SNMP versión 3 NO configurado en" `expr $numarchivos - $numcfged`
de $numarchivos dispositivos >> $report   → Nro. Ficheros que No emplean
version 3
grep -l "$SRCH2" * | awk -F':' '{print $1}' | sort -u >$f1; ls >$f2; diff $f1
$f2 | grep -i $cfgfileext | awk '{print $2}' | tee -a $report  → si "versión 3"
existe, con el "sort-u" deja una única instancia, lo guarda en una variable (fichero)
$f1, saca el listado de los routers que tengamos, los compara y finalmente nos
presenta los router donde NO se emplea esta versión (grep…)
rm -rf $f1 $f2 → borra los valores almacenados
```

Como acabamos de presentar, los comandos bash nos permiten realizar todo tipo de análisis sobre los archivos de configuración de estos dispositivos. La intención de haberlos presentado de forma integrada con la herramienta "ccsat" es que el lector pueda tomar como referencia la misma, y a través de sus propios desarrollos de módulos en bash pueda incrementar el nivel de evaluación hasta lograr el resultado deseado, sólo nos queda seguir adelante planteando qué más aspectos son básicos para esta tarea. A continuación presentamos algunos de ellos:

- Usuarios locales: Como medida básica para estos dispositivos, es importante contar con algún tipo de servidor RADIUS o TACACS que permita validar usuarios y a su vez almacenar registros de la actividad realizada. En el caso de ser TACACS es posible también regular qué tipo de comandos (por dispositivo) dispositivo puede ejecutar cada usuario y

llevar también el control de las ventanas de tiempo en las cuáles puede o no acceder. Debemos tener en cuenta, que como medida de seguridad (*disponibilidad de acceso de gestión*), en realidad es necesario el empleo de al menos un usuario local, pues si en algún momento falla la comunicación con el servidor, no existiría forma de conectarse con el router. Hay dos aspectos a evaluar sobre este o estos usuarios, el primero de ellos es que estén bien controlados, es decir quién se identifica con esa cuenta, contraseña robusta, control de privilegios, cambio de contraseña luego de emplearse en alguna oportunidad, etc. Y el segundo aspecto es la sentencia que se coloca en la configuración del router, en nuestro ejemplo podemos ver "*aaa authorization exec default group tacacs+ local*", esta línea nos indica que al solicitar autorización de acceso un usuario, primero se consultará el servidor tacacs (*tacacs+*), en el caso que este no responda, en segunda instancia permitirá la validación en local (*local*), si el orden fuera "*local tacacs+*", la secuencia sería a la inversa.

Cuando se verifica este parámetro, es posible también a través de comandos bash, comparar la existencia de usuarios locales con algún tipo de lista que deseemos considerar, en la cual se pueden incluir los usuarios triviales o predecibles de nuestra organización (cisco, admin, root…etc), es importante también considerar que los comandos bash empleados para este tipo de búsquedas contemplan el empleo de comodines del tipo: "*", "?", "> = <", los cuáles potencias más aún la verificación de existencias de este tipo de cuentas de usuario.

- <u>Contraseñas débiles</u>: En los router Cisco, lo que no se puede permitir es el empleo de password 7, pero también se puede realizar algún análisis más profundo, verificando por ejemplo con **John the Ripper** la fortaleza de las contraseñas tipo 5.
- <u>Servidor de autenticación externo (tacacs / radius)</u>: Como se comentó en la primera línea, es importante contar con este tipo de dispositivos. Este parámetro de control se agrega también, independientemente del primer punto, pues es frecuente que, a pesar de contar con este tipo de servidores, aún así existan usuarios locales.
- <u>Realización de backup</u>: El backup es la última medida que tenemos para recuperarnos de un incidente. El concepto de "disponibilidad", tal cual hemos mencionado con nuestra palabra "ACIDA" es un factor clave de la seguridad, de hecho los ataques de negación de servicio (DoS) tienen como objetivo atentar contra este concepto.

  La estrategia de backup, como hemos visto, debe estar rigurosamente establecida en un "Procedimiento de Gestión de copias de respaldo y recuperación" y aplicarse en detalle. Es muy frecuente que la gente de red, no le preste atención a esta actividad por lo robustos que son los dispositivos, pero por supuesto existen fallos intencionales o no que nos obligan a su recuperación. En general todos los dispositivos de red, independientemente de su fabricante, poseen un doble control de su funcionamiento; si está en servicio, en su memoria RAM está cargada la

configuración con la que está trabajando en ese momento, pero en su memoria no volátil está cargada (*o debería…*) su configuración de arranque. Esta doble memoria, tiene su fundamento en que el operador pueda realizar en remoto todo tipo de cambios y, una vez verificado su correcto funcionamiento, recién en ese momento puede estar seguro de guardar los cambios en memoria no volátil, si llegara a cometer cualquier error, sólo basta con reiniciar el dispositivo y este arrancará con la configuración que tenga guardada, sin afectar el cambio que se haya realizado.

Independientemente de que todos estos dispositivos almacenen sus configuraciones de arranque en memoria no volátil, como todos sabemos y hemos sufrido alguna vez, esta también falla, y por esta razón es que se deban realizar backups periódicos en servidores externos. Los dispositivos de red, también consideran este actividad como normal y están preparados para hacerlo. Dependiendo del fabricante, se presenta a través de diferentes comandos, pero en general la forma nativa de realizarlo es a través del protocolo "tftp" (Trivial File Transfer Protocol) que emplea el puerto UDP 69 y por ser UDP, no sobrecarga el tráfico de red. Si bien es un protocolo no seguro, se suele tener en cuenta que los segmentos de red de gestión deberían serlo, por lo tanto es frecuente hacerlo de esta forma, a estos comandos suele incorporarse también una línea en el cron del dispositivo para que lo haga con la periodicidad que se considere necesaria *(tengamos en cuenta que dependiendo del rol de cada router, su configuración es más estática o dinámica y sobre este rol es que se debe definir la periodicidad de los backups*).

Los dispositivos de red, como ya hemos mencionado se suelen configurar con ficheros de texto plano, por lo que el tamaño de los mismos no supera unos pocos kilobytes de tamaño. Existen también un gran número de aplicaciones que están diseñados para la gestión de backups, que facilitan y mejoran la tarea.

El concepto final que debemos remarcar es que, la actividad de backups es fundamental en los routers y que <u>sin lugar a dudas es un rol del área de seguridad el controlar su correcto funcionamiento</u>.

- <u>Envío de Logs a servidor de logging</u>: Toda la actividad de seguimiento y control de los routers queda almacenada en sus Logs. Cuando se emplean adecuadamente los servidores TACACS (y en menor medida también RADIUS), los mismos (TACACS) desempeñan perfectamente el papel de "servidores de Log" pues en realidad cada usuario que solicite acceso, si está habilitada la opción de "Accounting" dejará el rastro completo de cada comando que tenga permitido ejecutar, como así también los intentos de ejecutar cualquier acción que por TACACS tenga denegada, por lo tanto es uno de los mejores métodos de recolección de Logs y hasta de generación de alarmas. Por lo tanto, si estamos evaluando este parámetro de Logs en un router, y encontramos que no tiene configurado un servidor externo al

cual se envíen los Logs, pero sí tiene un servidor de TACACS, nuestra tarea será analizar con máximo detalle la configuración de este servidor.

En caso contrario, es necesario contar con un servidor al cual enviarle cada uno de los Logs que se establezcan como prioritarios. Describiremos el funcionamiento del sistema de Syslog en el capítulo siguiente.

El factor más importante que justifica este envío de Logs hacia dispositivos externos es que todo intruso experimentado, lo primero que realizará es el borrado de toda huella que permita seguir sus pasos y/o identificar lo que ha realizado, esta actividad una vez que ha comprometido un dispositivo y logrado escalar privilegios es relativamente sencilla, pero si los Logs se están enviando a otro dispositivo, para realizar este mismo borrado, debe primero eliminar las líneas de envío de Logs del dispositivo original (que ya ha enviado sus primeros logs de conexión del intruso) y luego intentar comprometer al servidor de Logs para borrarlos de él también.

A título de ejemplo, ponemos de manifiesto un ejemplo que demuestra contundentemente la importancia de esta medida. En una **red militar de alta seguridad**, para los dispositivos que procesaban información de carácter "Secreto" (*militarmente la información se clasifica como : pública, interna, confidencial y secreta, cabe mencionar que para decriptografiar la información secreta, en general es necesario presentar la clave de dos personas diferentes de forma concurrente*) se empleaba una impresora de matriz de punto con papel continuo, que imprimía cada uno de los Logs que se generaban en este servidor. La finalidad de tan extrema medida estaba justificada en que cualquier tipo de actividad anómala que se produjera sobre estos ficheros que contenían información "secreta" inmediatamente se imprimía en papel, por lo tanto si cualquier persona deseaba "borrar huellas" podría hacerlo sobre la información almacenada de forma electrónica, pero le resultaría imposible borrar una línea impresa en papel sobre un formulario continuo.

- Empleo de snmp v3: Este protocolo y su versión 3, lo hemos desarrollado en detalle en el libro "**Seguridad por Niveles**", por lo tanto no reiteraremos estos conceptos. En este punto, solo deseamos recalcar la necesidad de emplear esta versión por la importancia de Confidencialidad, integridad y autenticación que ofrece. Ante cualquier duda referirse al libro mencionado.
- Comunidades snmp de lectura: Por defecto al activar el empleo de snmp, vienen preconfiguradas las comunidades "**public**" para lectura y "**private**" para escritura. Todo intruso que desee exportar este protocolo, lo primero que intentará es analizar las mismas, por supuesto que es lo primero que hace cualquier herramienta de intrusión que trabaje con este protocolo. Si no se modifican estos nombres, ya tendrá acceso directo a nuestros dispositivos.
- Comunidades snmp de escritura: Ampliando los conceptos del párrafo anterior, merece la pena remarcar que la comunidad de escritura (write)

permite prácticamente la ejecución de todos los comandos de configuración que se deseen, si se sabe emplear este protocolo y un router permite su "escritura", podemos afirmar que no hay diferencia entre lo que podríamos ejecutar a través de línea de comandos con los máximos privilegios y lo que se peude ejecutar por medio del protocolo "snmp" pues dentro de la **MIB** (Management Information Database), que es el árbol que regula lo que se puede monitorizar, se encuentran la casi totalidad de los parámetros que soporta un router, pues justamente para ello fue diseñado este protocolo, por lo tanto, si puedo "sobre escribir" los mismos, estoy re configurando el funcionamiento del dispositivo.

Este parámetro debería estar deshabilitado si no se emplea, si se emplea debería estar muy justificada la razón (*en la mayoría de los casos es debido a que las herramientas de gestión de los diferentes fabricantes lo emplean*) y **bajo ningún punto de vista** permitir su uso en una versión anterior a la 3, pues en caso contrario, cualquier "escucha de tráfico", nos develará en texto plano el nombre de la comunidad y los parámetros que circulan por la red.

- Empleo de neighbor passwd en BGP, OSPF, RIP o ISIS: Estos protocolos dinámicos, tienen como misión, definir las mejores rutas por la cuales encaminar cada paquete a través de las interfaces de cada dispositivo. Cuando son empleados, generan todo una serie de paquetes, para publicar sus rutas, y definir caminos entre ellos (*recordemos la sección de BGP anterior y los conceptos de Router Reflector*). En toda gran red es imprescindible su empleo, cada administrador de red decidirá cuál de ellos empleará en sus diferentes zonas de red (*puede emplear más de uno de ellos simultáneamente*). Lo más importante a considerar es que a través de estos protocolos, toda la red adopta descisiones de encaminamiento de paquetes, por lo tanto, cualquiera que puede hacerse "partícipe" de este diálogo, en principio conocería toda la arquitectura de la red, y en segundo lugar podría alterar convenientemente los flujos para colocarse "entre medio" de la comunicación que desee. Este tema ya lo conocemos y se denomina "**ataque del hombre del medio**", y en el caso de estos protocolos, la mejor forma de describirlo es que el intruso luego de escuchar e interceptar convenientemente estos flujos, comience a generar paquetes que en definitiva transmitan el mensaje de "***yo soy la mejor ruta***". Si estos mensajes cumplen su objetivo, las tablas de ruteo de la interfaz atacada, decidirán que deberían enviar todos los paquetes que salen de ella hacia la dirección IP del router del intruso, el cual una vez que los reciba y previo a ejecutar todo lo que le convenga, los sacará nuevamente hacia el destino original, siendo totalmente "transparente su interceptación" si lo deseara, o peor aún, haciendo visible cuando le convenga causando el daño que desee.

  La primer medida para evitar este tipo de ataques es el empleo de algún tipo de medidas que puedan determinar fehacientemente que el emisor de estos mensajes sea alguien autorizado (***Que sea quien dice ser y no otro***:

Concepto de Autenticación), esto es lo que proponemos en este control, y la segunda medida es la que presentamos a continuación:

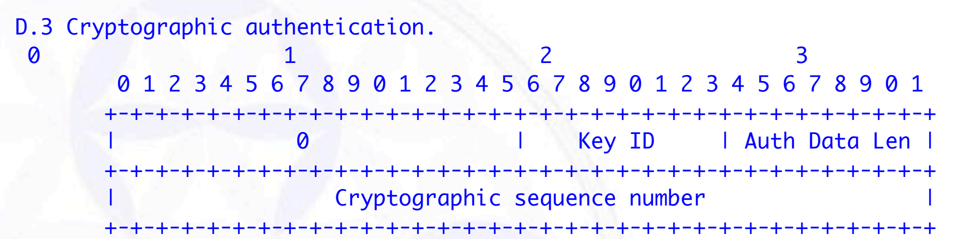
- Empleo de las últimas versiones de protocolos dinámicos, habilitando criptografía: Dependiendo del protocolo que haya seleccionado el administrador de la red, este ofrecerá mayor o menor cantidad de opciones de seguridad (*nuevamente ver libro "**Seguridad por Niveles**" para más detalle).* La versiones actuales de los mencionados protocolos, van adoptando poco a poco mejores medidas de seguridad.

  A continuación presentamos a título de ejemplo, algunas RFC que deberíamos tomar en cuenta para evaluar estas configuraciones para los protocolos OSPF y BGP.

  El protocolo BGP permite el empleo de criptografía desde prácticamente sus inicios, como podemos ver en la siguiente "RFC 2385: "Protection of BGP Sessions via the TCP MD5 Signature", existen varias actualizaciones y mejoras hasta llegar a la versión 4 que es la más reciente y podemos estudiarla según la "RFC 4271 A Border Gateway Protocol 4 (BGP-4)"

  En cuanto a OSPF, la versión que al menos debemos exigir es la versión 2 que está regulada por la "RFC 2328 OSPF Version 2"

  Por ejemplo, como presentamos a continuación, esta RFC en su punto "**D.3**", ya nos presenta una figura para que, dentro del mismo encabezado del protocolo, se puedan emplear sus campos para una autenticación segura:



```
D.3 Cryptographic authentication.
 0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |              0                |    Key ID     | Auth Data Len |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                 Cryptographic sequence number                 |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 18: Usage of the Authentication field in the OSPF packet header when Cryptographic Authentication is employed

  A lo largo del tiempo van apareciendo sucesivas mejoras para la seguridad de OSPF, algunas de ellas por ejemplo son: "RFC 5340 OSPF for IPv6" (*Si en nuestras redes ya se está planteando la migración hacia IPv6*). Otra RFC importante puede ser: "FC 6860 Hiding Transit-Only Networks in OSPF"

  Lo que deseamos poner de manifiesto en estas líneas y sin entrar en el detalle de seguridad de cada uno de estos protocolos dinámicos, es que es imprescindible aplicar medidas de seguridad a la hora de configurar protocolos dinámicos en nuestras redes pues son un potencial punto débil de alto impacto.

- <u>Acceso SSH</u>: Para la gestión de los dispositivos de red, si bien ya existen un sinnúmero de herramientas gráficas, en general todo administrador que lleve sus años gestionando estos dispositivos lo hará a través de línea de comandos o, al menos, seguramente conocerá su funcionamiento en detalle. Ya hemos tratado el tema de los protocolos seguros e inseguros en el libro "Seguridad por Niveles", en este punto sólo deseamos poner de manifiesto que no se puede seguir empleando "telnet" para la gestión de un router. Es muy (pero muy) poco probable que en la actualidad algún dispositivo de red o software de gestión no soporte la comunicación de forma segura empleando SSH, por lo tanto debemos exigir su uso.

  En general el empleo de ssh puede ser configurado de forma genérica o específica en cada interfaz. En nuestro router de ejemplo vemos "*transport input ssh*" que se encuentra dentro de la configuración da una interfaz vty "*line vty 0 4*", es decir, en este caso estamos restringiendo el empleo de acceso remoto por terminal virtual, exclusivamente para "entrada" (input) vía ssh, pero no hemos especificado qué sucedería para los accesos de consola o vía IP por alguna otra interfaz de gestión.

  Debemos ser extremadamente meticulosos en este control, pues cada fabricante aplica su metodología al respecto, e inclusive las diferentes versiones de sistema operativo dentro del mismo producto, también difieren, por lo tanto, a la hora de este análisis, es necesario verificar siempre TODAS las interfaces de acceso que posea el dispositivos y las opciones de control de acceso que ofrezca la versión de sistema operativo instalada sobre ese dispositivo en concreto.

- <u>Inhabilitado acceso telnet</u>: De forma similar al punto anterior, dependiendo del fabricante y versión de sistema operativo, en algunos casos es necesario deshabilitar específicamente este protocolo y en otros lo asume por defecto en el caso de no estar presente. Como dependiendo de estos factores, el tema puede ser ambigUo, es necesario controlarlo específicamente para esa configuración, y por supuesto garantizar que no esté habilitado.
- <u>Inhabilitado acceso ftp</u>: (no ftp-server enable): idem al punto anterior.
- <u>Empleo de servidor ntp</u>: Este punto que seguramente a primera vista del lector puede parecer secundario, es uno de los parámetros más importantes de seguridad en toda red. En primer lugar necesItamos poseer una **rigurosa jerarquía ntp**, según los niveles o "**Stratos"** que ofrece este protocolo y luego, incluir TODOS los dispositivos de red en la misma. Hoy en día es sumamente sencillo de establecer y hasta tomar como referencias los servidores de tiempo de carácter nacional o internacional que están disponibles, adoptando este reloj como "<u>estrato 0</u>" de la organización.

  En nuestra experiencia, la sincronización de tiempos de una red es fundamental a la hora de realizar cualquier actividad de forense, y tal cual

hemos presentado en puntos anteriores, mucho más si hemos trabajado bien y tenemos un sistema de centralización de Logs (*sin él la actividad forense suele ser imposible*). Nos ha pasado en reiteradas oportunidades que a la hora de realizar el seguimiento de incidentes, la secuencia de los Logs no estaba sincronizada y por ello, era extremadamente difícil seguir los pasos del mismo pues, los eventos se encontraban mezclados desde los diferentes dispositivos no pudiendo garantizar una línea de tiempo común. Este fallo de seguridad, incrementa y dificulta todo análisis forense, llegando al extremo de no poder esclarecer la incidencia.

- Empleo de ntp versión 4: Esta puede ser considerada como una medida complementaria a la anterior, pero nuevamente volvemos al tema de la importancia que en nuestras comunicaciones de red tenga la criptografía

  La versión 3 ya ofrece medidas criptográficas, pero si deseamos comprender o avanzar un poco más en estos conceptos debemos considerar la versión 4, que se presentó en el año 2010 con la **RFC 5905** "*Network Time Protocol Version 4: Protocol and Algorithms Specification*", recientemente (*en marzo de 2016*) se actualizó con la **RFC 7822** "*Network Time Protocol Version 4 (NTPv4) Extension Field*".

  Desde el punto de vista de la seguridad, esta RFC 5905, en su punto 15. "Security Considerations" presenta en los primeros párrafos los diferentes tipos de paquetes que un intruso podría inyectar a través del mal uso del protocolo, luego las limitaciones que asume el mismo haciendo referencia al empleo de un modelo **SSH** para la autenticación entre el cliente y el servidor ntp.

  Otro aspecto de importancia en la seguridad es que entre estas dos RFC aparece un nuevo concepto de autenticación por medio del empleo de clave pública haciendo uso de los encabezados en extensión. Hoy en día el empleo de certificados digitales es otro pilar de la seguridad y recién con la versión 4 es soportado este empleo de clave asimétrica por medio del campo "Message Code Authentication" (***MAC****..... no confundir con la misma abreviatura de direccionamiento de nivel 2 MAC: Medium Access Control*). Este esquema de MAC es empleado ya desde la versión 3 de forma simétrica, pero en la 4 amplía con Clave pública y privada.

- Empleo de Banners: Este otro aspecto que también puede parecer secundario es otra de las grandes sorpresas de la seguridad, pues en virtud de la ausencia de este tipo de mensajes ya se han librado varios delincuentes y han sido absueltos por la justicia al haber aducido que "*no tenían conocimiento de que estaban ingresando a una propiedad privada o que en ningún momento se les alertó que violaban ninguna ley*". Esta realidad, es totalmente cierta, y hasta en otros ámbitos de la justicia, también aplica con la misma lógica, es poco probable que puedan sancionarnos si ingresamos a un campo que no tiene vallas ni carteles que indiquen que donde estamos accediendo es propiedad privada o está negado el acceso, en el mundo digital sucede lo mismo.

Para prevenir este tipo de situaciones es que debemos considerar dos tipos de banner diferentes: El primero es antes que cualquier persona intente ingresar a un dispositivo, en el cual se le informa que el mismo es de nuestra empresa y sólo puede ingresar quien esté autorizado (al igual que un cartel físico en la puerta de entrada de un edificio), y el segundo es que una vez que se haya validado un usuario e ingresó al dispositivo (independientemente del privilegio con que lo haya hecho), se le advierte la obligación sobre la actividad que realice ya que la misma debe ser acorde a la autorización que posea, se le prohibe exceder cualquier tipo de derecho, y a su vez se le debe informar que está siendo monitorizado.

Con ambos mensajes, y ajustándolo específicamente a las leyes y normativas gubernamentales, se está configurando un dispositivo que advierte adecuadamente qué puede o no puede hacer cualquier persona que se presente ante él, y nos ofrece el respaldo legal necesario para poder actual ante la justicia por cualquier daño que nos ocasione el no cumplimiento de estos mensajes.

- <u>Deshabilitar interfaces sin uso</u>: Como todo dispositivo de red, las puertas de acceso al mismo son sus diferentes interfaces, es natural que si no se emplean estén cerradas, por lo tanto una muy buena práctica es que sólo las interfaces activas deben estar "UP", y las que no "Down" en las configuraciones.

- <u>Deshabilitar todo protocolo o servicio que no se emplee</u>: dependiendo del fabricante, modelo y sistema operativo, existen varios protocolos "clásicos" que pueden estar o no habilitados por defecto en una instalación estándar, ejemplo de ellos son bootp, CDP (Cisco Discovery Protocol), STP, DHCP, http-servers, boot-servers, ftp, telnet, etc.. Es nuestro trabajo, analizar qué dispositivo estamos evaluando y verificar cuál de ellos aplica.

- <u>Listas de Control Accesos</u> (**ACL**: Access Control List): <u>Este tema es uno de los puntos clave del análisis de seguridad de un router</u>, y también lo es el nivel de complejidad que pueden presentar las mismas y cómo impacta esta configuración sobre el resto de los parámetros, pues muchos de los parámetros que hemos presentado hasta ahora, provocarán mayor o menor grado de riesgo, en la medida que aplique adecuadamente una ACL sobre ellos.

  Casi podríamos afirmar que todos los parámetros de seguridad anteriores en mayor o menor medida dependen de una adecuada gestión de sus ACL, pues podemos permitir vecindarios (neighbor) que no empleen criptografía, si existe una ACL que nos obliga a comunicarnos exclusivamente entre dos extremos válidos, podemos emplear ntp versión 1, si existe una ACL que sea estricta sobre quién es el cliente y quién el servidor…… lo mismo aplicaría a telnet, ftp, usuarios, etc..

  Es muy difícil presentar una plantilla o una configuración segura de estas ACLs, nuestra recomendación es que se analicen con todo el detalle posible, una por una cada ACL que esté configurada, el primer objetivo de

este análisis es comprender los extremos de la comunicación del router que estamos evaluando, e identificar los flujos permitidos y los que no, para luego comparar estas medidas con el resto de las configuraciones.

Como hemos podido apreciar en esta sección, nuestro objetivo no ha sido hacer hincapié en la administración de routers, sino más bien en "cómo evaluar la seguridad de un router" sin ser el administrador del mismo. Este detalle es fundamental, pues de ser posible, deberíamos hacer un importante esfuerzo para separar esta actividad y que no sean los administradores de dispositios de red quienes tengan que vela por su seguridad. Cuando este rol lo asume una sola persona, en general encontraremos grandes brechas de seguridad, y nuestra experiencia al respecto no nos deja la menor duda al respecto, pues en su operación del día a día, la gente de red necesita "mantener el servicio" a toda costa, y es frecuente que le soliciten nuevas conexiones, puertos accesos, comunicaciones, mensajes, etc… y su prioridad será satisfacer las mismas sin afectar el servicio. A lo largo del tiempo estas medidas se suman o van quedando en el olvido y será por allí por donde aparecerá el futuro incidente casi con seguridad.

Para que estos puntos débiles se minimicen, o sean detectados oportunamente, es que la mejor solución es la segmentación de tareas, y que sea el área de operación y planificación quienes se encarguen del servicio y el área de seguridad quien vele o controle su adecuada parametrización.



6. Plataformas / Infraestructuras de Seguridad en Red

6.1. Presentación

Hasta ahora hemos desarrollado los primeros niveles del modelo de capas y de forma complementaria a lo presentado en el libro "**Seguridad por Niveles**" fuimos ampliando conceptos de protocolos, routing y switching. En este capítulo presentamos una serie de despliegues que son de utilidad en el trabajo de Seguridad de nuestras redes. Muchos de estos despliegues pueden ser considerados como plataformas, infraestructuras, appliances, desarrollos de software e inclusive como un conjunto de medidas de seguridad. Nuestra intención de presentarlas en esta capítulo es que una vez que ya hemos comprendido los dos niveles más importantes de una red (Enlace y red) ahora podamos aplicar diferentes productos u ofertas del mercado para ampliar nuestro trabajo de seguridad, por esa razón es que los hemos incluído en este capítulo, aunque es cierto que algunos de ellos no respondan estrictamente al título de "Plataforma" o "Infraestructura".

6.2. Control y filtrado de accesos

Dentro de esta sección, es importante diferenciar las actividades que podemos llevar a cabo desde un Firewall que es el dispositivo por excelencia para esta actividad de lo que también nos ofrece hoy en día un router, que tal cual hemos puesto de manifiesto varias veces, su potencia actual le permite asumir funciones que no son necesariamente su rol principal. Por eso es que dividiremos aquí la presentación de ambos dispositivos.

6.2.1. Firewalls.

Los conceptos y definiciones sobre Firewalls (en adelante FW) ya han sido desarrollados en el punto 6.3. del libro "**Seguridad por Niveles**". Manteniendo la filosofía de este nuevo libro, en este capítulo desarrollaremos desde el punto de vista del área de seguridad de la empresa, cuáles son los aspectos que debemos evaluar, siempre con un enfoque transversal e independiente de las diferentes áreas de operación, y en este caso al igual que en los routers, es importante poder contar con una visión independiente, respecto a los responsables de "Operación" de Firewalls y lo que analizaremos en esta sección que está orientado a los responsables de "Gobierno" de la seguridad, que deben velar por el mantenimiento del nivel de seguridad, en este caso de los responsables de esta herramienta.

En la actualidad existen varias definiciones, conceptos y funcionalidades para analizar un FW, para nosotros explicar este concepto o idea es sencillo, pues sólo nos interesan como FWs de red, es decir, aquellos que están en capacidad de trabajar en los niveles 3 y 4 del modelo de capas, nada más.

De lo desarrollado en "**Seguridad por Niveles**", únicamente nos detendremos en dos conceptos:

- Política permisiva.
- Política restrictiva.

Este tema será uno de los más frecuentes con el que nos cruzaremos en nuestras redes, pues veremos reglas excesivamente "amplias" que abren acceso a grandes rangos de direcciones o de puertos, lo cual es una muy mala práctica.

Otro tema que hemos detectado con mucha frecuencia en varias redes, es la mala gestión de los FWs, actividad que se evidencia en lo siguiente:

- Ausencia de una metodología estricta de gestión de reglas.
- Ausencia de sistemas de "trazabilidad" (*o ticketing*) en cada regla.
- Falta de control de sus Logs.
- Poca concienciación en optimización de reglas.
- Bajo empleo de herramientas de gestión automatizadas (*y donde existen, no se las explota adecuadamente).*
- Poca supervisión externa de los mismos (*no se puede ser juez y parte*).

<u>¿Qué puntos debemos controlar especialmente</u>?

a) Estrategia de despliegue de Firewalls.

El despliegue de Firewalls debe responder a una visión global de la totalidad de la infraestructura, de no ser así se presentan <u>zonas "grises</u>" que redundan esfuerzos, gastos o dejan brechas sin proteger.

Para evitar este tipo de sucesos es que es de suma importancia que exista una <u>estrategia Global</u> de la empresa (*tema que encontramos que no es así en varias redes*).

Los indicadores más claros de la existencia de esta estrategia son el claro conocimiento de la situación de los FWS por parte del área de Ingeniería y Planificación (*Haciéndose evidente cuando sólo desde aquí nacen estos despliegues*). La presencia de proyectos de despliegue centralizados, la existencia de planos globales, la centralización de su gestión, la existencia de procesos de seguimiento, monitorización (auditoría) y optimización de FWs, etc.

Todos estos aspectos deberían ser analizados previamente de forma documental, para luego poder abordar la parte más técnica de gestión de los mismos.

b) Dimensionamiento.

Tal vez por la falta de visión global (estrategia) es que se encuentre muy a menudo la existencia de errores en el dimensionamiento del despliegue de FWs, tanto por defecto, como por exceso.

Este tema, ciertamente es muy difícil de cuantificar, pues no se trata de tener pocos FWs con miles de reglas, ni cientos de ellos con baja actividad.

Lo que se debe evaluar aquí (*casi subjetivamente*) es la impresión que deja el despliegue de los mismos, bajo las siguientes ideas: Zonas protegidas y/o desprotegidas, sobre carga de "Hits"/CPU o memoria de los FWs, excesiva latencia en la red o pérdidas de paquetes, fallos de tunelización o demasiada visibilidad entre segmentos de red, aplicación de políticas muy dispares entre los diferentes FWs, etc.

c) Responsabilidades, obligaciones y distribución de funciones sobre los FWs.

¿Está claramente documentado cada uno de estos roles?

¿Existe un flujo estricto para el Alta, Baja o Modificación (ABM) de reglas?

¿Se cumplen ambos procesos?

¿Hay personal "imprescindible"?

¿Las figura involucradas son "Juez y parte"de las tareas?

d) Gestión de Firewalls.

Se debería analizar (*junto al responsable de cada dispositivo*) lo siguiente:

- cómo se conecta al FW
- La claridad de sus mapas, direcciones, cuentas, contraseñas.
- Qué tipo de protocolos emplea.
- Si respeta o no lo documentado en cuanto a autenticación y control de accesos.
- Qué privilegios posee.
- Si emplea o no herramientas que faciliten la gestión.
- Qué hace con los backups de sus configuraciones y políticas, si los encuentra con agilidad, si conoce cómo recuperar alguno de ellos.
- Qué sucede cuando esta persona está ausente.

- Cómo lleva adelante (*en la práctica*) el flujo de cambios de configuraciones
- Si responde o no a un ticket que lleve todo el histórico.

e) Auditoría de Firewalls.

- ¿Se realiza esta actividad de forma periódica y por personal ajeno a su operación?
- ¿Hay evidencias, informes, acciones de mejora?
- ¿Poseen las herramientas adecuadas?

f) Controles de rendimiento y "hits" de reglas.

- ¿Se realiza algún tipo de control sobre la ocurrencia o "hits" que suceden sobre sus reglas?
- ¿Se han adoptado acciones de mejora sobre este control de "hits"?
- ¿Existe algún mecanismo de control del rendimiento de las reglas de estos FWs?

g) Configuración de políticas.

- ¿La configuración de las políticas, responde a alguna metodología?
- ¿Es de aplicación homogénea en todos los FWs?
- ¿Responde a algún tipo de Workflow?
- ¿Está documentado el empleo de objetos, redes, rangos, identificadores, etc? (como "abreviaturas" y acrónimos que involucren varios elementos)

h) Configuración de Logs.

- ¿Qué tipo de eventos se "Loguean"?
- ¿Se realiza un mantenimiento adecuado de sus Logs?
- ¿Se realiza alguna explotación de los mismos?
- ¿Hay alguna constancia de esta explotación?
- ¿Se identifican acciones de seguimiento y/o mejora sobre este control de Logs?

i) Envío de Logs.

- ¿Se están enviando a un servidor externo?
- ¿Se explotan los mismos desde este servidor?
- ¿Se realiza algún tipo de correlación de Logs?
- Existe alguna política de borrado, rotación y/o compresión de Logs?

j) Sistema/metodología de gestión de reglas (proceso, flujo, autorizaciones, constancias, registros).

- ¿Existe una metodología documentada?
- ¿Se cumple con ella?
- ¿Es adecuada la responsabilidad de creación y/o modificación de reglas?
- ¿Existe una clara jerarquía de autorización sobre las reglas?
- ¿Queda constancia histórica de estas acciones?
- ¿Se puede asociar cualquier regla con su ciclo de vida?

k) Reglas holgadas y ajustadas.

Para esta evaluación, es importante dedicar un tiempo a analizar y comprender (*junto al administrador del FW*) los diferentes objetos, grupos y redes que están definidos, luego seguir el orden de alguna secuencia de reglas, verificando que las mismas respondan con la máxima exactitud a la función que deben cumplir, evitando dejar abiertas más direcciones y/o puertos o servicios que las necesarias (*tanto origen como destino*).

l) Estrategias de optimización de reglas.

En rasgos generales, todo FW sigue una lógica secuencial de sus reglas, es decir por cada paquete que ingresa, lo comienza a verificar desde la primera, segunda, tercera…. "n" regla; si ella aplica, entonces cumple con lo que se indique, sino pasa a la siguiente y así hasta llegar al final donde si existe un "DROP" elimina el paquete, en caso contrario, lo dejará pasar. A todo esto se suma también el seguimiento de determinadas acciones, protocolos, secuencias, estados, etc.

Al entrar en producción, puede haber sido diseñada la mejor forma de configurar este FW, pero inexorablemente a medida que va creciendo su política (*cosa muy corriente y dinámica en estos dispositivos*) su lógica inicial se ve afectada ocasionando cronológicamente una merma en su rendimiento, que será mayor o menor, sobre la base de la cantidad de cambios sufridos y la lógica que haya dispuesto su administrador, pero este es un hecho concreto que degrada todo FW.

Independientemente de una buena gestión, la única forma de ir revirtiendo este proceso es por medio de acciones, análisis, herramientas, y hasta pruebas cuya finalidad sea la "Optimización" del FW.

En este control, lo que deberíamos evaluar es la existencia y aplicación o no de estas estrategias (*no que sean realizadas voluntariamente por determinadas personas, sino como un proceso debidamente documentado*).

m) Medidas adoptadas de optimización (histórico, registros, acciones, resultados, etc.).

En relación directa con el punto anterior, ahora sí, se verificará la existencia de estas evidencias que dejen por sentado las medidas que se hayan adoptado o no.

n) Interfaces gráficas de gestión.

En el caso de que los FWs empleen interfaces gráficas para su gestión, estas suelen presentar la característica que sobre las mismas se permite el acceso a más de FW, desde la misma se pueden ejecutar cambios y luego "inyectarlos" en los FWs respectivos.

Lo que se desea evaluar de estas herramientas gráficas es que respondan a las metodologías de autenticación y control de accesos reguladas por los procesos correspondientes, que se administren por medio de protocolos seguros, que si desde ellas se almacenan las copias de seguridad de los FW, entonces que también se exporten a un servidor determinado, que respondan a medidas de bastionado, etc.

A su vez este tipo de herramientas suelen ofrecer funcionalidades para generar informes o realizar actividades de monitorización automáticas, en estos casos, debemos verificar qué tipo de acciones se realizan sobre las mismas.

o) Acceso al dispositivo (FW).

En este punto, se deben evaluar las metodologías que se emplean para acceder a los mismos, desde dónde, quiénes pueden hacerlo, la existencia o no de medidas de control de acceso y las cuentas que se emplean para ello.

p) Empleo de herramientas para la gestión de Firewalls.

En muchas redes se emplean este tipo de herramientas que van más allá de las interfaces gráficas de gestión. Este punto se refiere concretamente a herramientas diseñadas para la "optimización" y auditoría de FWs, (*Ej.: Firemon, Tuffin, Algosec*). En los casos en que se estén empleando, verificar

qué explotación se realiza sobre las mismas, haciendo especial hincapié en la adopción de medidas que evidencien un ciclo de vida eficiente para estos dispositivos y con que nivel de detalle y profundidad se están empleando (*alcance de la herramienta*).

q) Informes, reportes, estadísticas, acciones (de estas herramientas).

Analizar los resultados obtenidos con los mismos, calidad de los informes, detalle de los mismos, acciones de mejora, etc.

r) Medidas de resguardo y recuperación de configuraciones.

La dinámica de las reglas o políticas de un FW hace que sus medidas de backup deban ser adoptadas con especial atención, pues resulta extremadamente difícil volver a configurar un FW si no se cuenta con Backup actualizados, por esta razón es que se presenta como un control detallado desde el primer ciclo de esta auditoría.

Se debe verificar que los administradores conozcan al detalle el funcionamiento de los backups y el conjunto de acciones necesarias (*protocolares, jerárquicas y técnicas*) para recuperarlos ante cualquier tipo de incidencia.

6.2.2. ACLs en routers.

Como indicamos al presentar el punto 6.2 de "Filtrado y control de accesos", los routers hoy en día, en virtud de la potencia de los mismos, tienen la capacidad de "mimetizarse" con un FW y en muchos casos es difícil diferenciarlos. Lo importante es que conceptualmente no son lo mismo, y tampoco su diseño es pensado para esta actividad, por lo tanto, el primer aspecto a considerar aquí es que si bien un router puede implementar "listas de control de acceso" básicas (*sólo filtrando direcciones IP*) y avanzadas (*también puertos*) este, en general, no tiene capacidad (*ni daría su rendimiento*) para mantener el control de sesiones, en particular sobre el protocolo TCP (*aunque existen tareas similares sobre UDP*).

Un Firewall (FW) Sí puede hacerlo, y ésta hoy en día es una de sus principales fortalezas.

El control o seguimiento de sesiones es la mejor forma de poder detectar, procesar y decidir qué se puede o debe hacer sobre:

- Ataques de negación de servicio puntuales y/o distribuidos.
- Ataques de inundación.
- Barridos o escaneos de direcciones, puertos o máquinas.
- Actividades de Fingerprinting o Footprinting (*reconocimiento de redes y sistemas*).

- Actividades o código malicioso entrante y saliente (*Virus, troyanos, spam, etc…*)
- Falsificación de direcciones y puertos origen y destino.
- Falsificación de credenciales de acceso.
- Ataques gota a gota.
- Intentos de elevación de privilegios.
- Ataques de ruptura de contraseñas y usuarios.
- Análisis y determinación de redes y sistemas comprometidos.
- Reconstrucción (o forense) sobre actividad sospechosa.

Nada de lo anterior puede (*o debería….)* **hacerse desde un router.**

¿Qué consideraciones debemos tener en cuenta para diferenciar el rol de un router con ACLs y un FW?:

a) Segmentación de funciones.

Al intentar realizar tareas de enrutado (*nativas de un router por operar en nivel 3*) y tareas de protección (*nativas de un FW*) en un solo elemento o dispositivo, no se da cumplimiento a uno de los principios básicos de seguridad que es el de "Segmentación de funciones".

La administración de dispositivos, según los perfiles de acceso, no permitiría la existencia de dos (*o más*) perfiles cuyas obligaciones y responsabilidades puedan ser excluyentes; es decir, sobre un router sería imposible definir un perfil que tenga capacidades de modificar rutas y no ACLs, y otro diferente que pueda hacerlo sobre las ACLs y no sobre las rutas. Tampoco podría ser independiente de esto quien administre su sistema operativo y/o kernel.

Esta falta de segmentación presenta serios problemas en la gestión de la seguridad, pues quien habilite cualquier ruta, a su vez será (*o podrá ser*) quien aplique los permisos respectivos para facilitar el acceso o no a las mismas.

Adicionalmente, cabe destacar que, si bien solemos confiar en los empleados de la empresa, el 80% de los problemas de seguridad, según estadísticas, provienen de los propios empleados, que como conocen el detalle de la arquitectura y sistemas, son los de más alto impacto para la organización…….

En esta situación, sería este mismo usuario o perfil quien tenga todas las potestades para borrar absolutamente todas las huellas y no dejar ningún rastro.

b) Protección de infraestructuras propias, clientes, empresas y otros proveedores.

En las grandes redes se suele producir un doble conflicto:

- Proteger las propias infraestructuras (*como red de tránsito*).
- Proteger los destinos de esa comunicación.

Por ejemplo en el caso de la interfaz de salida a Internet de una gran red, esta es la puerta de entrada y salida, por lo tanto, desde la misma, se debe contemplar un conjunto de medidas (*o reglas*) que permitan la protección de la infraestructura propia y de los destinos de la comunicación (*que en muchos casos son proveedores, clientes, otras empresas, socios de negocio, etc.*).

Hay que tener en cuenta que un router de frontera hacia Internet por ejemplo, no posee sólo dos interfaces; suele tener configuradas varias decenas de ellas, cada una conectado a segmentos diferentes. Sobre cada uno de ellos, si no se lleva algún tipo de control de sesiones o gestión de reglas (*al detalle*), se está facilitando la posibilidad de "mezclar" estos flujos.

Otro problema que sucede en grandes redes es que, por no llevar el control de los flujos de clientes o empresas (*entrantes y salientes),* sus dispositivos o servidores, pasaron a formar parte de listas negras de Internet (*con el coste o multas que ello ocasiona*), pues al hacer NAT o por falta de control, las direcciones IP que aparecían como conflictivas eran del rango de esa organización (*algunas veces administradas por la empresa o cliente final y otras por la propia organización*).

A esto podemos sumar como ya hemos comentado, que en muchos casos las cuentas de estos clientes y/o empresas pueden ser de "alto impacto", y por lo tanto no puede, ni se debe, dejar pasar el tráfico desde y hacia ellas sin ningún tipo de control, e insistimos, este control no es sólo puntual en la "interfaz o equipamiento del lado del cliente o empresa externa" sino que debe responder a una visión "Global de la seguridad" y poder tener una visión completa. Por ejemplo hay vulnerabilidades sobre determinados tipos de túneles que deben ser seguidas desde ambos extremos simultáneamente en, de otra forma no pueden ser analizadas.

c) Bastionado.

En más del 80% de los diagnósticos de seguridad de red que hemos realizado, se ha detectado falta de actualización sobre los routers de la red.

Esto es perfectamente comprensible, pues a la hora de actualizar un dispositivo, su hardware, software, sistema operativo, kernel o poner un parche se debe realizar previamente una prueba de maqueta, lanzar todos los controles necesarios, los backups, la vuelta atrás, hacer pruebas y dejar

por escrito su recuperación del servicio al 100%, evaluar la acción de mejora, proponer este "feedback", etc…

Sobre los elementos de producción esto debería estar "PROHIBIDO" en todas las organizaciones.

Por el alto coste de un router crítico, es altamente probable que no se cuente con maquetas de este tipo, y por su nivel de complejidad, es también probable que este tipo de modificaciones no se realice con la periodicidad con que se debiera, y por esta razón en general TODOS ellos presentan fallos de seguridad por falta de actualizaciones y por lo tanto poseen más o menos vulnerabilidades, pero casi TODOS poseen alguna.

No sucede lo mismo en el caso de un FW, pues este tipo de acciones son cotidianas y cualquier organización posee un ejemplar en maqueta o un firewal virtual, o al menos en zonas sobre las que una prueba y validación de una actualización no causaría impacto. Por esta razón, es mucho más sólido poseer un FW que un router de esta magnitud directamente expuesto.

d) Excesiva carga de trabajo.

Si bien en algunas organizaciones se están empleando routers en determinadas interfaces como reemplazo de un FW, podríamos afirmar, gracias a los diagnósticos realizados en las distintas grandes redes, que el volumen de reglas que tienen configurados es excesivamente alto (*varios cientos de reglas y hasta miles*), lo que supone una carga adicional de trabajo que puede ser evitada. A su vez, no cabe duda que la optimización de este tipo de reglas es mucho más eficiente en FWs que en routers.

e) Diseño de hardware y software.

Un router está diseñado para poseer una altísima capacidad de procesamiento (*en ciclos de CPU*) para poder gestionar sus paquetes con máxima velocidad.

Un FW está diseñado para poseer una alta capacidad en el control de "ventanas" de envío y recepción (*en particular sobre el protocolo TCP*), por lo que cuenta con velocidad en ciclos de CPU, alta memoria RAM para mantener millones de sesiones abiertas, cada una de ellas con cuatro ventanas: secuencia de envío y recepción origen, y secuencia de envío y recepción destino.

Cuando se intenta mezclar ambas capacidades en un solo dispositivo, impacta en uno u otro lado.

f) Escasa escalabilidad y flexibilidad al medio plazo (*y nula al largo*).

La posibilidad de hacer NAT y filtrado en un solo dispositivo (Por ejemplo: router de frontera hacia Internet), impactará al medio/largo plazo pues se está realizando NAT 444, es decir, un doble NAT (*primero en el lado del cliente, y luego en la salida hacia Internet)*, pero en el medio plazo, éste será NAT 464, NAT 664, y más adelante no habrá NAT (pues todo será IPv6).

En ese momento se debe tener en cuenta que el nuevo esquema de direccionamiento permitirá miles de miles de millones de direcciones IP internas visibles desde todo Internet (*cosa que hoy es el punto de protección más robusto de todas nuestras infraestructuras, por ejemplo de direcciones IP privadas*).

g) Carga de un router frontera.

En la actualidad un router de salida hacia Internet se emplea para:

- Protocolos de enrutado dinámico exteriores e interiores (*alta carga de trabajo*)
- NAT
- Enrutado en todas sus interfaces
- Control y gestión VRF (Virtual Routing Forwarding)
- Control y gestión de VPN (Virtual Private Network)
- Control de claves criptográficas
- Encriptado de paquetes (en los casos en que aplica)
- Sincronización de tiempos
- Generación, análisis y envío de sus logs
- Generación y análisis de traps SNMP (Single Network Monitor Protocol)
- Autenticación y control de acceso de sus usuarios

No sería una buena decisión sobre este tipo de dispositivos, la sobrecarga de tareas que implica analizar cada uno de los paquetes para adoptar o no medidas de filtrado.

Resumiendo este punto, el concepto clave que nos debe quedar, es que las ACLs en un router son necesarias, y hasta podríamos considerar imprescindibles, pero lo que no debemos aceptar es la línea de pensamiento que propone que **a través de las mismas se puede reemplazar el empleo de FWs**, esta no es su misión.

6.3. Supervisión / Monitorización / Alarmas

Nuestra experiencia al respecto es muy positiva en general en toda red de gran envergadura, no siendo así en redes de menor tamaño. En general todas las grandes redes, poseen mecanismos robustos para esta actividad. En casi todas ellas existen con mayor o menor nivel de madurez, algún tipo **NOC** (Nework Operation Center) que dedica desde algunas horas al día hasta otros que ofrecen servicio 24x7, y en cada uno de ellos tiene integrado los dispositivos y plataformas de red que han sido determinados como críticos para la organización.

El aspecto sobre el que sí podemos centrarnos, es el el "Flujo y categorización" de alarmas e incidentes de seguridad. Debemos diferenciar el concepto de "**NOC**: Network Operation Center" del de "**SOC**: Security Operation Center", pues este último sí debería abocarse exclusivamente a seguridad, mientras que el primero no. La cuestión está en que no todas las redes tienen recursos para un SOC (y en muchos casos, tampoco se justifica que lo tengan), en estos casos evidentemente algún tipo de tareas relacionadas a seguridad deberían recaer sobre el NOC.

Sea cual fuere la situación (con o sin SOC), nuestro objetivo debería conducirnos a obtener una visión clara sobre:

¿Qué hace este personal si detecta alguna anomalía en la red, cuyos parámetros puedan esta relacionados con un incidente de seguridad?

Ejemplos típicos o indicadores de ello son:

a) Incremento anómalo de ancho de banda.

b) Saturación del ancho de banda.

c) Caídas secuenciales de dispositivos.

d) Propagación abusiva de un determinado patrón de tráfico.

e) Modificaciones sensibles del flujo de tráfico de nuestros DNSs.

f) Incremento llamativo del volumen de Logs.

g) Mensajes anómalos en los Logs de elementos de red.

h) Alarmas en bases de datos, procesadores, módulos de memoria.

i) Alteración de rutas.

j) Fallos en los sistemas de señalización.

Este tipo de ocurrencias, pueden ser indicios de algo en relación con incidentes de seguridad. En principio podemos indagar acerca de si están o no tipificados estos casos, ¿Existen evidencias de este tipo de anomalías?, en segundo lugar deberíamos analizar si:

a) ¿Existe un procedimiento ante estos casos específicos?

b) ¿Se conocen los pasos a seguir?

c) Dentro del workflow de este centro, ¿está contemplado un “ticket” (*es decir: varios*) para temas relacionados a seguridad?

d) ¿Está tipificado o categorizado este flujo para incidentes de seguridad?

e) ¿Se conoce la jerarquía, niveles de escalado o cadena de comunicación para estos casos?

f) ¿Cómo se abre, verifica, mantiene y cierran estas incidencias?

Este tipo de tareas <u>sí</u> son las que hemos verificado que presentan flancos en la mayoría de las redes. Por esta razón es que en nuestra trabajo de revisión de seguridad, deberíamos organizar y dedicar espacios de tiempo para nuestra visitas al:

- NOC
- SOC
- Centros de supervisión de red

Que existan en nuestra red.

6.4. Centralización y explotación de Logs

Una de las acciones que mayor esfuerzo requiera , tanto desde el punto de vista del personal de red, como a nivel corporativo es justamente la implantación de plataformas de centralización de Logs, pues una vez planificado y lanzado este trabajo, debe involucrar a la mayoría de las áreas de la organización. Hoy en día debemos referirnos a estas como **SIEM**: Security Information and Event Management.

En realidad el concepto de SIEM viene de una combinación de dos soluciones (o definiciones) anteriores:

- **SIM**: Security Information Management
- **SEM**: Security Event Management

Al unir ambas ideas aparece, tal vez más robusta, la posibilidad de "<u>correlar</u>" (*o correlacionar*) eventos de seguridad. Hoy en día estas implementaciones son de uso frecuente, y podemos presentar como modelo tres proveedores:

- EnVision de RSA.
- Arcsight de HP.
- Splunk (*Puede discutirse si es o no un SIEM…)*

Nuestra experiencia es que cuando se está desplegando o ya está en producción este tipo de plataformas, desde el punto de vista de seguridad deberíamos verificar dos aspectos de la misma:

1) El nivel de implantación y explotación alcanzado.

2) El nivel de seguridad en la gestión de la plataforma.

El trabajo, nuevamente lo desarrollaremos desde el puesto del administrador de la plataforma o desde donde esta persona pueda acceder a la misma, y desde allí analizaremos la actividad, para lo cual desarrollemos a continuación un poco de ambos aspectos:

1) El nivel de implantación y explotación alcanzado.

Los indicadores del estado de implantación podemos medirlos en base a:

- Tiempo de puesta en producción de la herramienta.
- Recursos dedicados a la misma.
- Análisis de prioridades sobre elementos críticos que deban enviar Los a la plataforma.
- Cantidad de ellos que en la actualidad estén enviando Logs.
- Gestiones en curso para nuevas integraciones de envíos de Logs.
- Desenvoltura del administrador en el manejo de la herramienta.
- Tipo de consultas, vistas, informes y estadísticas definidas.
- Informes generados.
- Explotación de la plataforma: descubrimientos, elevación, evolución, seguimiento, acciones de mejora que hayan generado estos informes.
- Por último, un detalle que no debemos pasar por alto es la actualización a la versión más reciente.

2) El nivel de seguridad en la gestión de la plataforma.

El acceso a la plataforma debe estar realizándose a través de https hacia la interfaz web de acceso, nos debería pedir inmediatamente la validación de acuerdo a la imagen que figura a continuación (*tomaremos como ejemplo el producto de RSA Envision, que en la actualidad se denomina "RSA Analytics", pero podríamos seguir esta secuencia de acciones desde cualquier otro producto*).

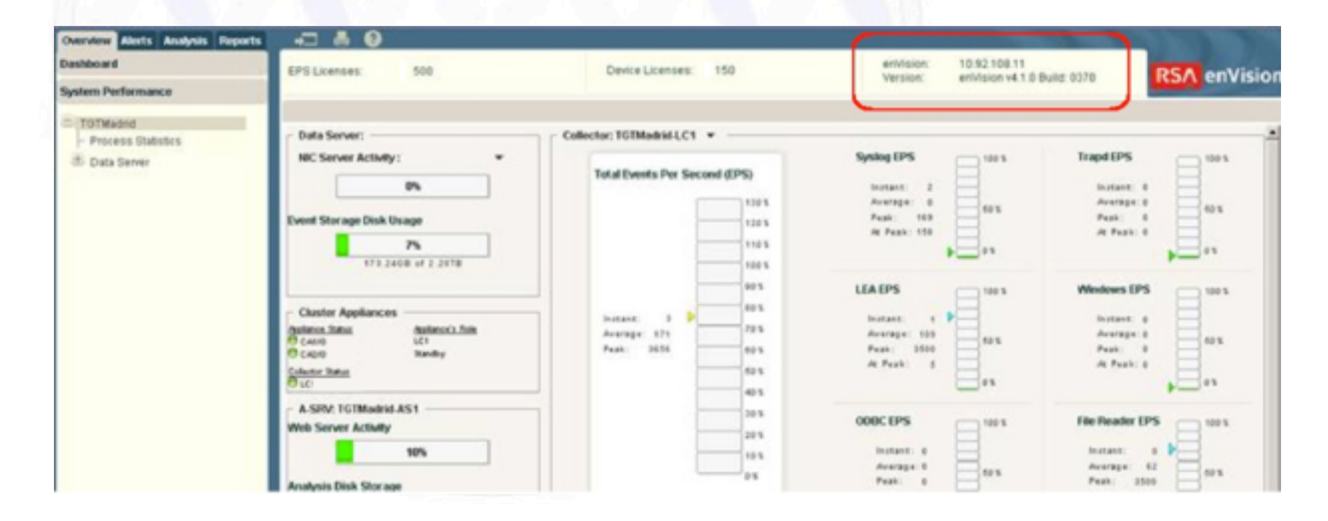


Imagen 6.1 (Ejemplo de versión en RSA enVision)

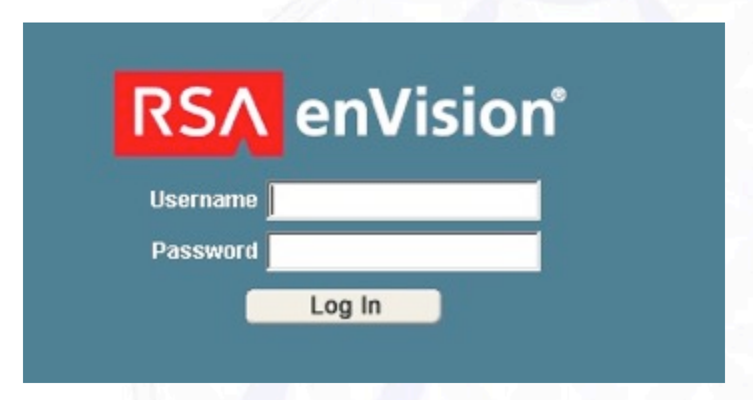


Imagen 6.2 (Ejemplo ingreso usuario RSA enVision)

Durante esta validación, podemos verificar que no se realice con el usuario por defecto "Administrator", cosa que evidentemente debería estar prohibido en el procedimiento de Gestión de Accesos y no debería emplearse, sino que se debe acceder por medio de usuarios personales.

Como segundo paso podemos solicitar nos muestre las cuentas de usuario que están dadas de alta en la plataforma, para verificar que no sean excesivas y que a su vez existan algunas (y no sólo Adminsitrator). La imagen que se presenta a continuación nos muestra esta ventana.

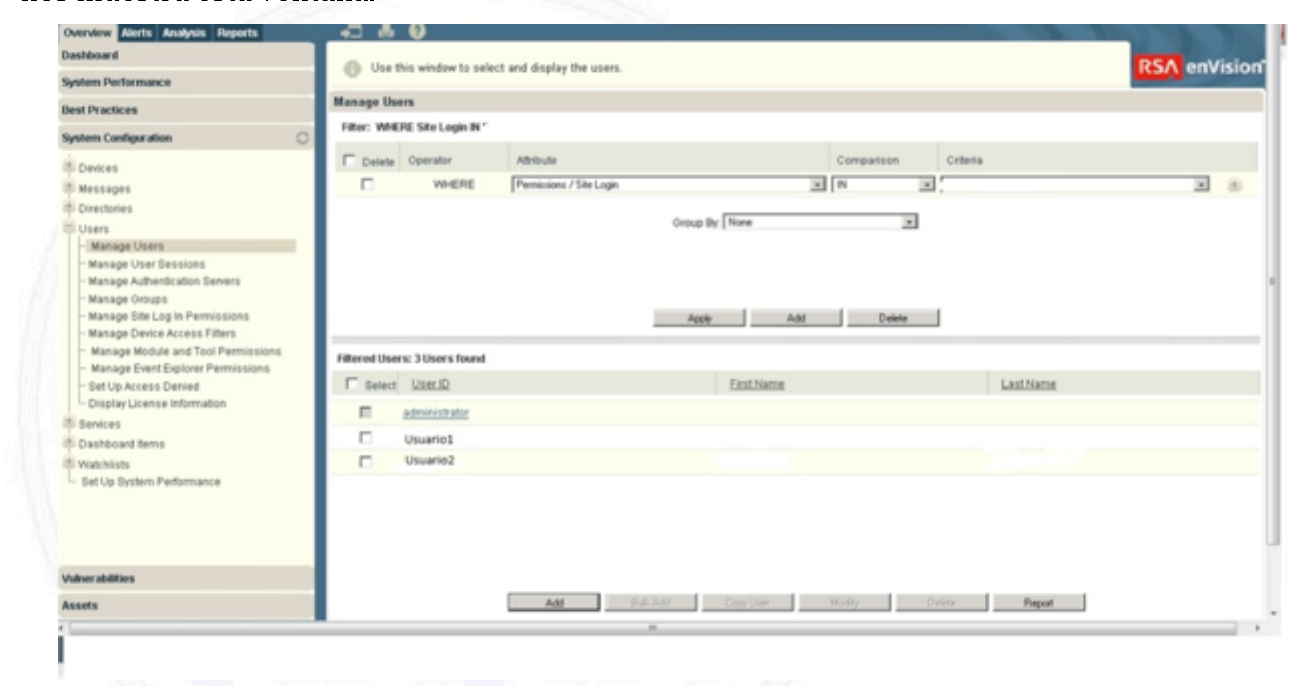


Imagen 6.3 (Ejemplo de cuentas de usuario)

Nuestro último control al respecto puede ser la consulta sobre los “**login**” de usuarios sobre esta plataforma en un período de tiempo (Podemos filtrar por el “Sting: UserSession”), en esta consulta nos interesa observar que no sean excesivos, que no se esté empleando “Administrator”, y que no aparezcan “Fails” más allá del normal error de equivocarse alguna vez en la validación.

En la siguiente imagen podemos apreciar esta consulta.

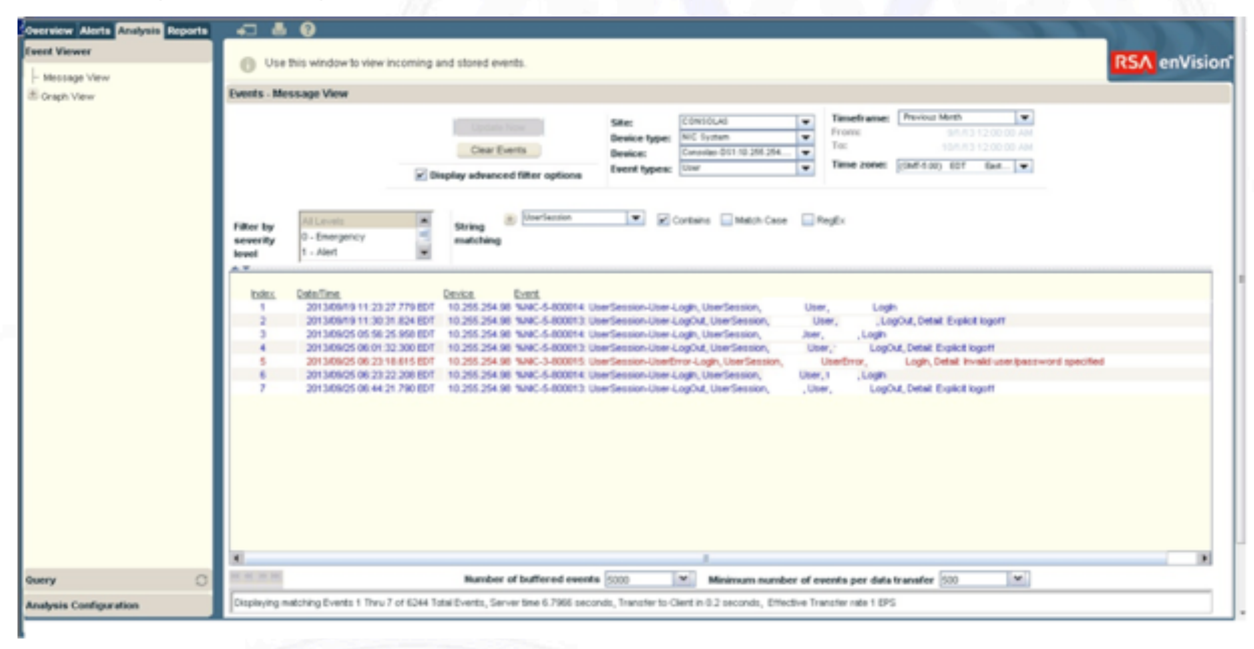


Imagen 6.4 (Ejemplo de Logs de usuario)

Si disponemos de tiempo suficiente, una actividad importante es poder verificar que se esté implantando de forma segura y “**ajustada**” el acceso de cada dispositivo que envía Logs hacia aquí. Para ello, el trabajo radica en elegir uno o más dispositivos cliente de este SIEM, analizar su arquitectura con el plano correspondiente, seguir la ruta de estos envíos (saltos en routers), y luego en los Firewalls y/o ACLs en router correspondientes corroborar que las reglas sean verdaderamente “**ajustadas**”. Sobre este punto por ejemplo, aspectos clave son:

- El que envía Logs (la fuente) es un dispositivo concreto, no un “rango” o segmento de red, por lo tanto la regla debería ser una sólo IP origen. Las excepciones que pueden presentarse sobre este tema, son por ejemplo que exista un segmento claramente identificado y ajustado de red donde se encuentran varias fuentes de Logs (Ej: Core de routers críticos).
- El puerto normal de envío de Logs, es el estándar de “Syslog”: **UDP 514**. Sólo debería encontrarse este como destino.
- Existen excepciones de envíos a este puerto, que se denominan “File Reader” en EnVision, por ejemplo cuando el “**Colector**” (que es quien debe recolectar los Logs) necesita obtenerlos de sistemas particulares, caso “Microsoft Exchange”, en estos casos necesita hacer empleo del protocolo “**sftp**” a través del puerto TCP 22 de forma “bidireccional”, por lo tanto pueden ocurrir este tipo de excepciones, siempre y cuando se encuentren debidamente

documentadas. Otro tipo de ellas son hacia **ODBC** (Puertos 1433 y 1434), también hacia sistemas propietarios como el caso de los Firewall Check Point con los puertos lea 18184 y 18210, el envío y recepción de **snmp** con puertos UDO 161 y162. En máquinas Windows recientemente se ha habilitado otra alternativa de consultas a eventos por http o https (TCP 80 y 443). En cualquier caso lo que nos interesa es que en ninguno de ellos existe la necesidad que la regla de filtrado sea "generosa u holgada", SIEMPRE podrá (o deberá) ser puntual ←→ puerto TCP 22, → puerto TCP 1434, → TCP 443, etc.

Lo que se presenta a continuación, son varios ejemplos que reflejan la falta de atención sobre los Logs recibidos en este Log Server desde un FW Juniper, que nos pueden servir de ejemplo sobre parámetros que deberíamos considerar a la hora de centralizar Logs Como podremos apreciar no es adecuado que se esté generando este tipo de tráfico dentro de la red, si estos Logs se estuvieran revisando, evidentemente se debería haber solucionado este tema.

Logs recibidos del firewall-juniper

```
Time      Filter  Action  Interface      Protocol          Src Addr              Dest Addr
01:17:33  gestion   D       local          ICMP          10.10.119.90          10.10.119.90
01:17:32  gestion   D       local          ICMP          10.10.119.90          10.10.119.90
01:17:31  gestion   D       local          ICMP          10.10.119.90          10.10.119.90
01:16:12  gestion   D       local          ICMP          10.10.119.90          10.10.119.90
…….
```

Se trata de su propia Interfaz:

```
group SERVICIO {
        type external;
        local-address 10.10.119.90;
        neighbor 10.10.119.89 {
            export export-SERVICE;
            peer-as 649xx;
```

NOTA: No es normal en absoluto que este tipo de tráfico con la misma IP origen y destino se esté generando.

```
00:25:53  gestion   D       local          ICMP          11.11.11.2            11.11.11.2
00:25:52  gestion   D       local          ICMP          11.11.11.2            11.11.11.2
00:25:51  gestion   D       local          ICMP          11.11.11.2            11.11.11.2
00:25:50  gestion   D       local          ICMP          11.11.11.2            11.11.11.2
               ………
               policy-options {
                   prefix-list routers {
                       10.3.9.92/30;
                       …….. 
                       11.11.11.0/30;

00:23:48  gestion   D       local          ICMP          12.12.12.2            12.12.12.2
00:23:47  gestion   D       local          ICMP          12.12.12.2            12.12.12.2
00:23:46  gestion   D       local          ICMP          12.12.12.2            12.12.12.2
00:23:45  gestion   D       local          ICMP          12.12.12.2            12.12.12.2
………
00:20:27  gestion   D       xe-0/1/0.1116 ICMP           12.12.12.2            12.12.12.2
```

```
00:20:26  gestion   D      xe-0/1/0.1116 ICMP          12.12.12.2              12.12.12.2
00:20:25  gestion   D      xe-0/1/0.1116 ICMP          12.12.12.2              12.12.12.2
00:20:24  gestion   D      xe-0/1/0.1116 ICMP          12.12.12.2              12.12.12.2
………..
00:11:08  gestion   D      xe-0/1/0.1116 ICMP          11.11.11.2            11.11.11.2
00:11:07  gestion   D      xe-0/1/0.1116 ICMP          11.11.11.2            11.11.11.2
00:11:06  gestion   D      xe-0/1/0.1116 ICMP          11.11.11.2            11.11.11.2
00:11:05  gestion   D      xe-0/1/0.1116 ICMP          11.11.11.2            11.11.11.2
……………
```

NOTA: De los párrafos anteriores, no es normal que se esté generando este tipo de tráfico ICMP con la misma IP origen y destino, si bien no se puede verificar que esto esté saliendo o no a la red, su generación es anómala.

```
04:26:45  seg-router-core A local  UDP          10.111.31.9          224.0.0.2
04:26:41  seg-router-core A local  UDP          10.111.31.9          224.0.0.2
04:26:36  seg-router-core A local  UDP          10.111.31.9          224.0.0.2
04:26:32  seg-router-core A local  UDP          10.111.31.9          224.0.0.2
…………
```

NOTA: No es frecuente que un multicast lleve por encima protocolo UDP.

```
04:24:04  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:24:03  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:24:02  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
……………
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:24  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
04:23:23  seg-router-core A local  UDP          10.111.31.9        10.111.31.10
```

NOTA: De …………..se repite 10 veces por segundo………………..

```
08:01:12  pfe       D      ae2.32        UDP           181.64.127.182        10.116.130.45
08:01:10  pfe       D      ae2.32        UDP           181.64.127.182        10.116.130.45
08:01:09  pfe       D      ae2.32        UDP           181.64.127.182        10.116.130.45
07:57:06  pfe       D      ae2.32        UDP           181.64.127.182        10.116.130.45
```

NOTA: De ………… se repite constantemente……………

6.5. Detección / Prevención / Mitigación

En este punto, hemos agrupado algunas herramientas diferentes que cumplen estas funciones y desarrollamos a continuación.

6.5.1. IDSs/IPSs (Sistemas de Detección / Prevención de intrusiones)

Este tema en cuanto a su desarrollo teórico, nuevamente, recurriremos al libro "**Seguridad por Niveles**", en su punto "7.15. Sistemas de detección de Intrusiones" se describe al detalle estos elementos.

En cuanto a los aspectos que nos interesan en nuestras revisiones de seguridad, lo que más evidente se hace en estas plataformas es lo siguiente:

- Generación de reportes y/o informes.

  Hemos verificado en general que en las redes que conocemos, existe una gran carencia en esta tarea y, verdaderamente es la razón de ser de este dispositivo, pues si no genera resultados, no sirve de nada. Su funcionamiento principal justamente, no es para forense, es decir reactivo (*aunque también es de suma utilidad para ello*), sino justamente la "detección temprana", por lo tanto si se está explotando adecuadamente, sin lugar a dudas debe estar alertando sobre uso anómalo de donde esté escuchando, si estas alertas no generan acciones, entonces ¿Para qué sirven?

- Nivel de actualización de sus reglas.

  Como bien conocemos, día a día aparecen vulnerabilidades, debilidades, errores, virus, troyanos, gusanos, bugs…….. por esta razón es que todos los proveedores de estas herramientas poseen equipos de trabajo abocados a investigar estos patrones de conducta y diseñar la respuesta adecuado. Una herramienta de este tipo, si no se actualiza periódicamente, pierde gran parte de su utilidad.

- Existencia de reglas personalizadas.

  En muchos casos, se presenta el hecho, que se es consciente de una determinada vulnerabilidad, pero que es imposible de solucionar (*porque el software no lo soporta, no se puede instalar el parche correspondiente, etc*), lo mejor en estos casos es poder contar al menos con una alarma en tiempo real de cualquier intento de explotación de la misma. Para ello, todas estas herramientas ofrecen la posibilidad de diseñar reglas locales y personalizadas que detecten estas conductas.

  Un trabajo serio sobre IDSs, siempre debe llevar aparejado este tipo de reglas locales o personalizadas.

- En el caso de IPSs, lo que más nos interesa es el tipo de respuesta.

  Un IPS, justamente está diseñado para "Prevenir" que lo que se ha "detectado" siga avanzando en nuestra red, y pueda adoptar acciones concretas para "Bloquearlo". Estas acciones concretas pueden presentar el peligro que un intruso también las "detecte", y explotándolas adecuadamente, logre dejar fuera de servicio una red, justamente porque el IPS decidió bloquear ese tráfico. Ya se

conocen bastantes casos de este tipo de hechos, por lo tanto, lo que aconsejamos aquí es que se profundice acerca de cuál es el sentido con el que se está bloqueando tráfico, y por supuesto cuántas veces este bloqueo dio resultado (nuevamente, recurriremos a los registros, informes y estadísticas).

6.5.2. Plataformas de mitigación/detección

Para explicar de forma gráfica estas herramientas, recurriremos al producto PeakFlow/TMS de Arbor. Esta plataforma está presentada por el fabricante Arbor Networks y el paquete comprende dos herramientas diferentes:

- Peakflow
- TMS: Threat Management System

En algunas redes, sólo poseen PeakFlow como una herramienta de supervisión y monitorización de tráfico, es cierto que desde la misma manualmente se pueden configurar medidas para minimizar ciertos patrones de tráfico, pero el concepto de "Mitigación" efectivo pasa por medio de TMS. Su lógica la podemos describir mejor a través de las siguientes imágenes.

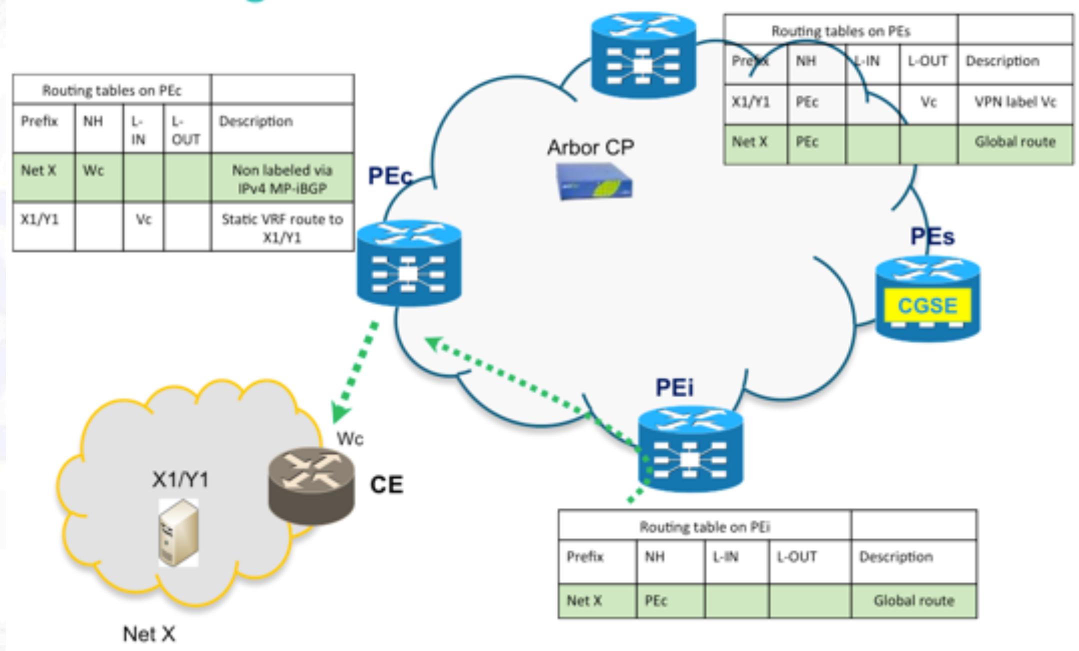


Imagen 6.5 (Lógica de PeakFLow - imagen 1)

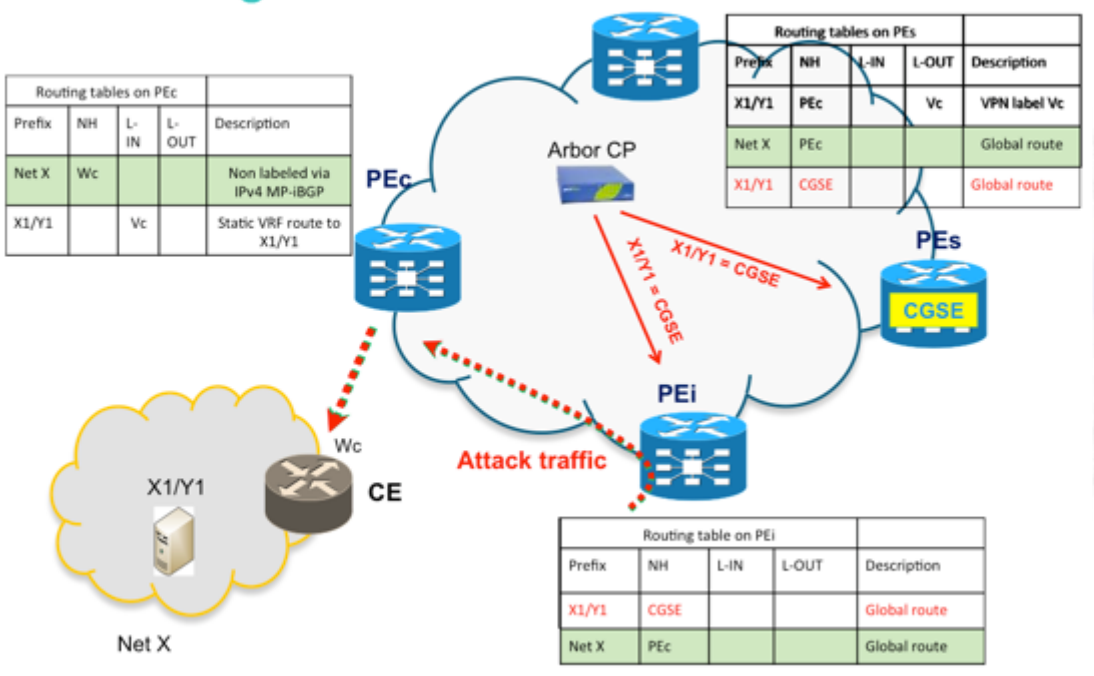


Imagen 6.6 (Lógica de PeakFLow - imagen 2)

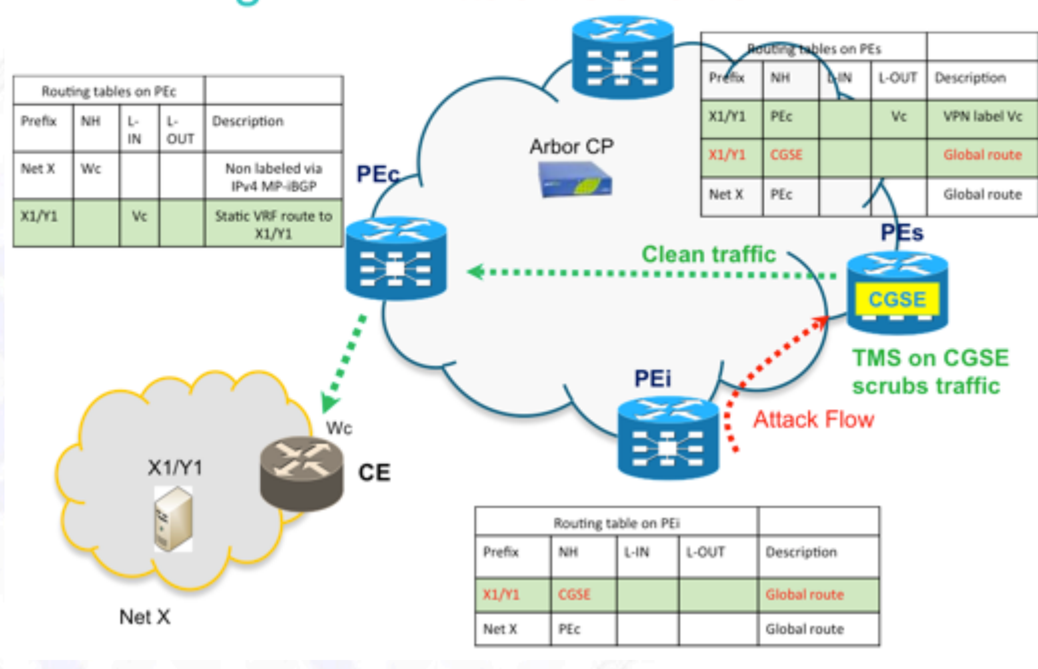


Imagen 6.7 (Lógica de PeakFLow - imagen 3)

La implementación de esta plataforma en una red real podemos verla como se presenta a continuación.

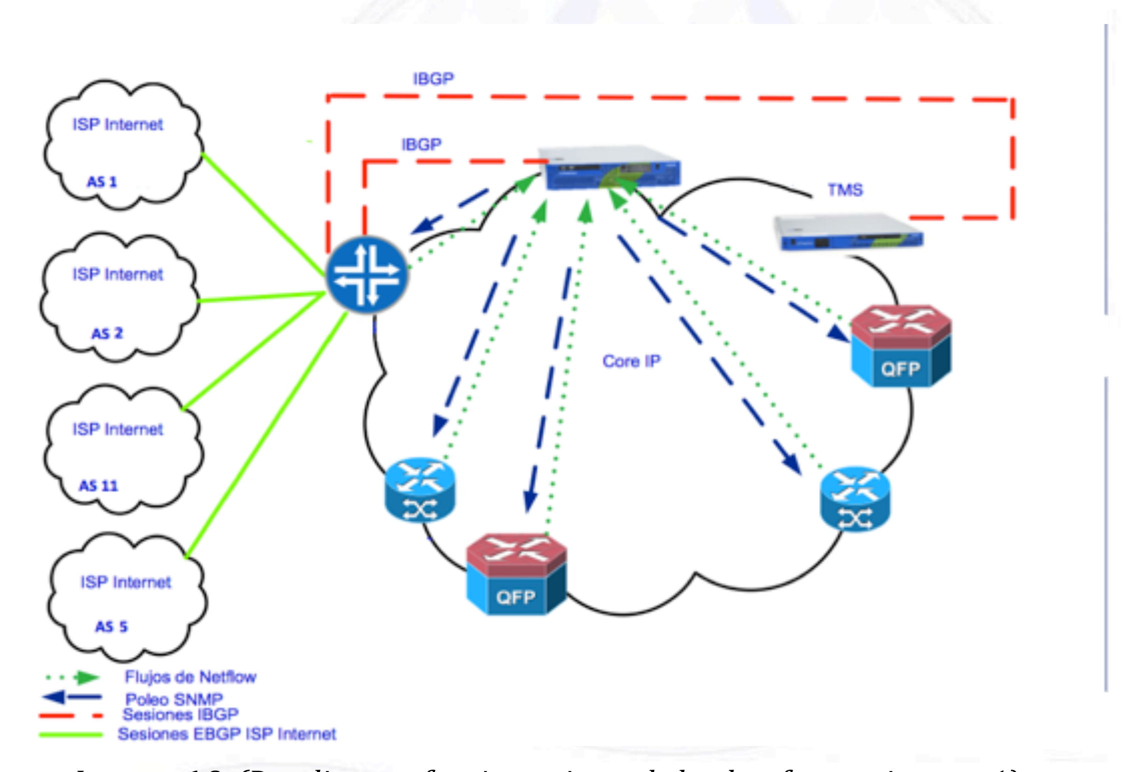


Imagen 6.8 (Despliegue y funcionamiento de la plataforma - imagen 1)

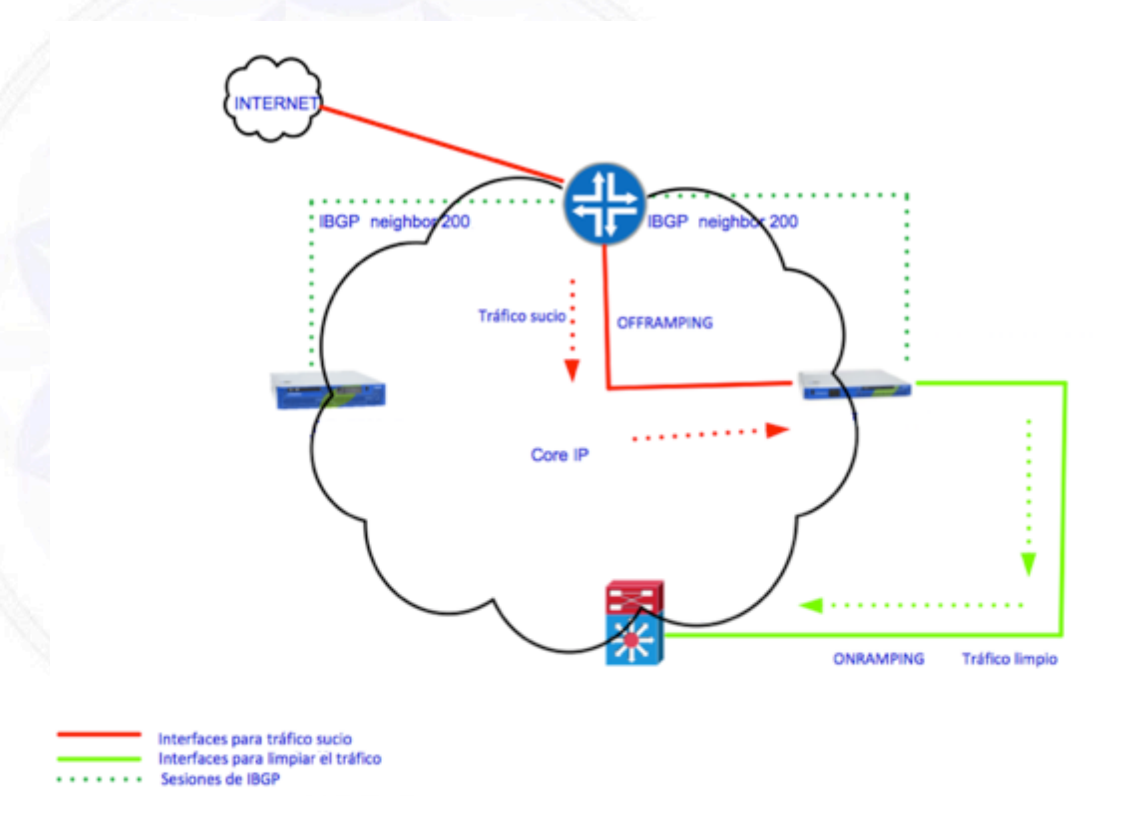


Imagen 6.9 (Despliegue y funcionamiento de la plataforma - imagen 2)

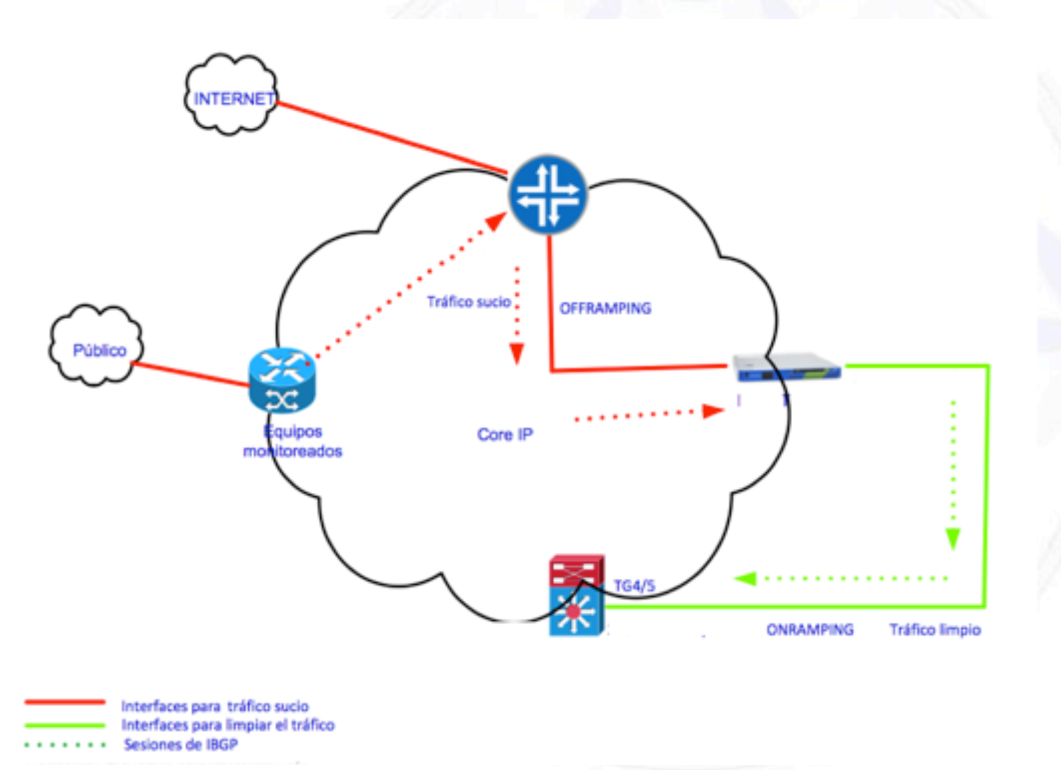


Imagen 6.10 (Despliegue y funcionamiento de la plataforma - imagen 3)

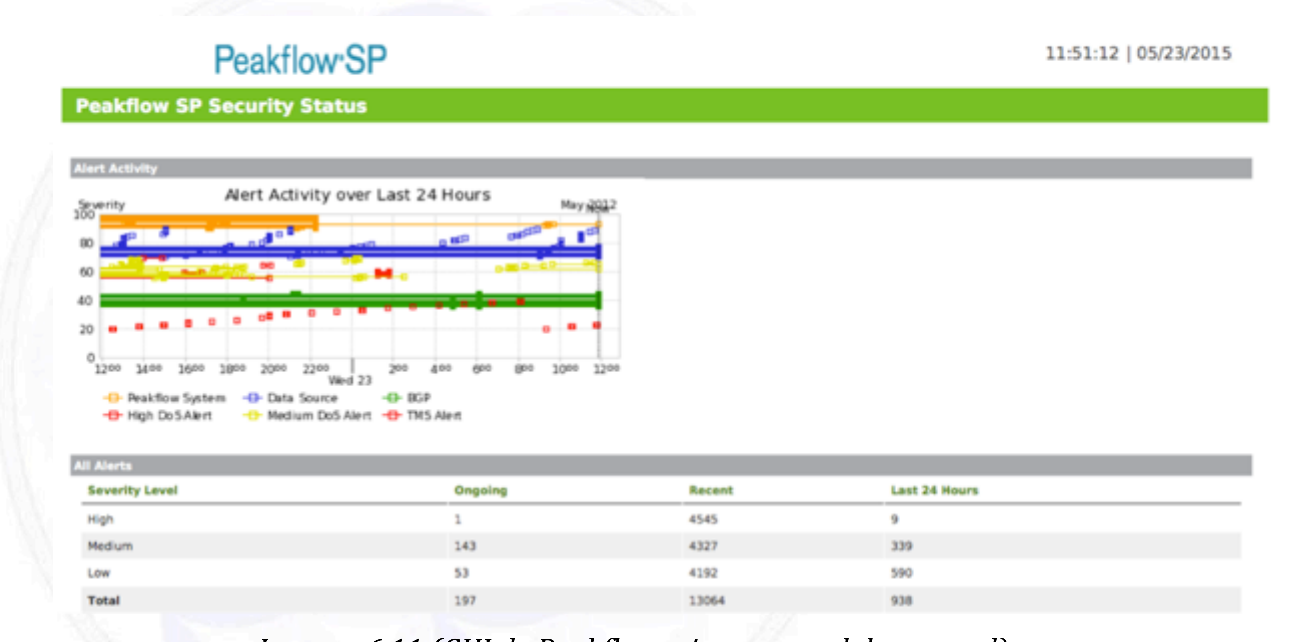


Imagen 6.11 (GUI de Peakflow – imagen real de una red)

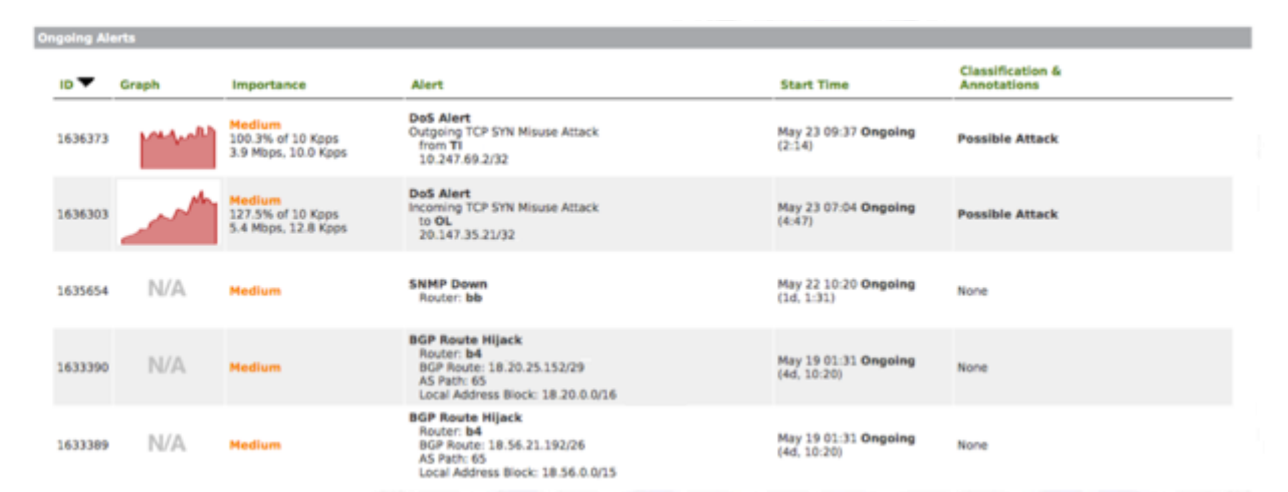


Imagen 6.12 (GUI de Peakflow – imagen real de una red)

Sobre esta plataforma, nos centraremos en los aspectos que ya hemos ido desarrollando en las anteriores, y los indicadores del estado de implantación podemos medirlos en base a:

- Tiempo de puesta en producción de la herramienta.
- Recursos dedicados a la misma.
- Desenvoltura del administrador en el manejo de la herramienta.
- Tipo de consultas, vistas, informes y estadísticas definidas.
- Informes/reportes generados (Acciones concretas de mitigación).
- Explotación de la plataforma: descubrimientos, elevación, evolución, seguimiento, acciones de mejora que hayan generado estos informes.

6.6. Infraestructuras para la resolución de nombres.

En cuanto a las redes de servicio y gestión de las diferentes organizaciones, el tema de la resolución de nombres en la actualidad suele estar a cargo de las plataformas **DNS** (Domain Name Service), nuevamente en cuanto a su desarrollo teórico, recurriremos al libro "**Seguridad por Niveles**" en su punto "7.1. DNS (Domain Name System)", en el libro este tema está desarrollado con máximo nivel de detalle.

Para nuestro trabajo y despliegue, independientemente de los conceptos de "Autoritativo" y "Caché", debemos conocer que en todas ellas podemos encontrar al menos dos tipos de DNSs:

- Para empleo de la propia organización o corporativo (los que usan todos los ordenadores de los empleados de la empresa).
- Los de empleo de clientes y empresas de la propia organización.

Dentro de estas dos categorías podemos encontrarnos varias formas de implementación e inclusive de integración o fusión de ellos.

Estos dispositivos, tal cual se presenta en la teoría, fueron, son y serán blanco de todo tipo de ataques, pues sin ellos sería prácticamente imposible navegar por Internet, y quizás tampoco por la red de cualquier gran empresa.

La historia de estos dispositivos, podríamos presentarla como que nace de la mano del desarrollo Open Source "**Bind**", fue el mejor, y aún mantiene una posición respetable, si bien hay que admitir que la competencia privada ha dedicado un esfuerzo admirable y hoy en día está ofreciendo productos de la forma de "Appliance" con los que es difícil competir desde el mero software, lo que sí es cierto es que casi todos ellos tienen parte del motor de Bind. El detrimento innegable de Bind es que es un hecho que su administración sigue siendo muy "estricta" en cuanto al empleo de línea de comandos y muy poca gente conoce al detalle sus pormenores, causa por la cual es muy raro encontrarlo actualizado y bien configurado. Sea cual fuere el motivo, es cierto, como dijimos que los productos comerciales le han ido ganando mercado y hoy en día en el mercado podríamos presentar que existen dos líderes sobre el tema:

- Nominum
- Secure 64

En general hemos podido verificar que gran parte de las grandes redes ya están alineadas con esta decisión, y también es una realidad, que existe una importante diferencia entre la labor de un DNS Autoritativo, contra el de un DNS Caché (*que son los que se pueden saturar con mayor frecuencia*), por esta razón es que nos encontraremos aún con muchas instalaciones de Bind, cosa que si está debidamente administrado es totalmente normal.

Seguridad en DNSs y DNSSec (Domain Name System Security Extensions)

La organización jerárquica del Sistema de Nombres de Dominio y su trabajo clave en Internet , como ya mencionamos, lo posicionan como uno de los mayores blancos de ataque.

La funcionalidad del sistema DNS es resolver nombres ← → direcciones IP. (sin esto es imposible navegar).

Desde su nacimiento en los años 80 hasta hoy, sus mayores debilidades (y continúan siéndolo) son los engaños sobre esta asociación (pues son su única función).

Esta infraestructura inexorablemente debe entrar en contacto con cualquier usuario de Internet dejando el puerto 53 (TCP y UDP) abierto. Su única protección pasa por:

- Bastionar robustamente cada host (hardening) de esta infraestructura.
- Mantener siempre actualizados sus versiones de SSOO y aplicaciones.
- Monitorizar su actividad y configuración permanentemente.
- Colocar las barreras en los elementos que no necesariamente estén visibles.
- asegurar la integridad de sus registros de información (y este es el punto clave).

Estimación: Para la información que se posee hasta ahora sobre estos productos, es probable que este último punto no se encuentre aún en un estado de avance considerable al momento de la publicación de este texto.

Desde principios del 2000 empezó a presentarse este conjunto de especificaciones sobre DNSSec, pero recién en 2008, se consolidó con la aparición de la **RFC 5155** "Hashed Authenticated Denial of Existence" conocida como DNSSec3.

El punto clave de toda esta propuesta pasa por la implementación de "firmas" de zonas a través del empleo de certificados digitales.

Con esta estrategia, se asegura la "Integridad" de las zonas de todos los servidores y a su vez las respuestas que se ofrecen a las solicitudes, solucionando con ello el problema más crítico de este servicio.

6.7. Balanceo de carga.

Esta actividad, se refiere a la técnica empleada para repartir el trabajo entre diferentes procesos, procesadores, software o hardware. En nuestro caso, para el análisis de redes, donde más aplica es en repartir "tráfico". Esta actividad se realiza mediante algoritmos que facilitan esta división de la forma más exhaustiva posible.

El balanceo de carga en grandes redes (describiéndolo *sólo desde el punto de red*) es una técnica bastante frecuente, en particular para servicios que requieren alto tráfico como es el caso de plataformas DNSs, Servicios de CGNAT (Carrier Grade Network Address Translation), dispositivos virtuales de red (FWs, LDAP, etc). Al igual que las plataformas DNS, son objetivos muy interesantes para intrusos pues estos dispositivos justamente concentran grandes flujos de tráfico, y

volviendo al tema de la sección anterior, si los DNSs son blanco de ataques, mucho más lo será una plataforma que centraliza todos los DNS (*si se está aplicando balanceo sobre este servicio*).

La técnica que más se aplica en telecomunicaciones es bajo el concepto de "cluster" (*no es el concepto clásico de cluster*), en esta idea, se definen nodos, de los cuáles uno de ellos es el "Front end" y el resto el "Back end" que es hacia donde se reparten los flujos de tráfico.

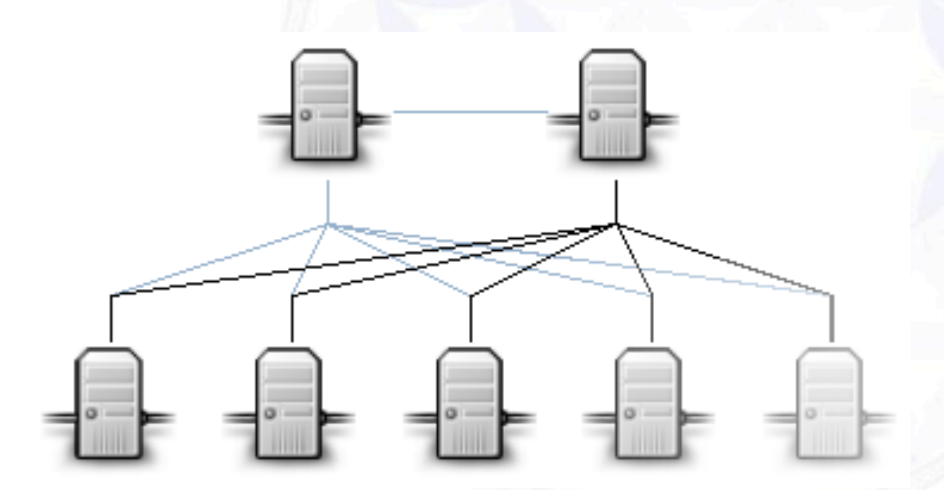
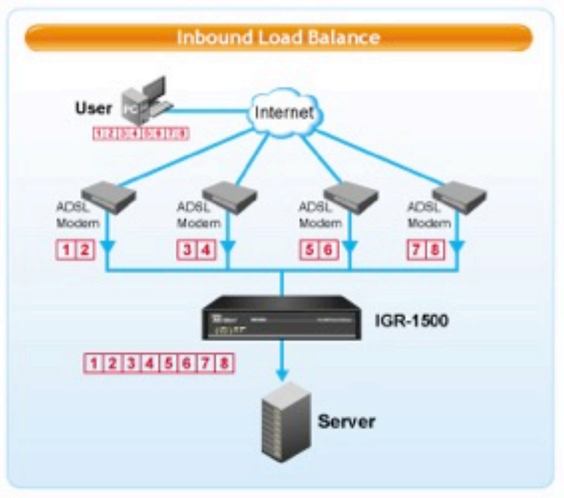


Imagen 6.13 (Esquema de lógica de balanceo)

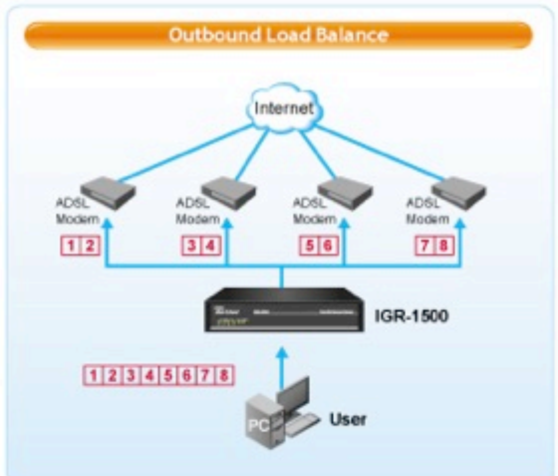
Las características más destacadas de este tipo de cluster son:

- Escalado: Se puede ampliar su capacidad fácilmente añadiendo más ordenadores al cluster.
- Robustez (Disponibilidad): Ante la caída de alguno de los nodos del cluster, el servicio se puede ver mermado, pero mientras haya otros en funcionamiento, éstos seguirán dando servicio.

Existen diferentes formas y flujos para el balanceo de cargas.







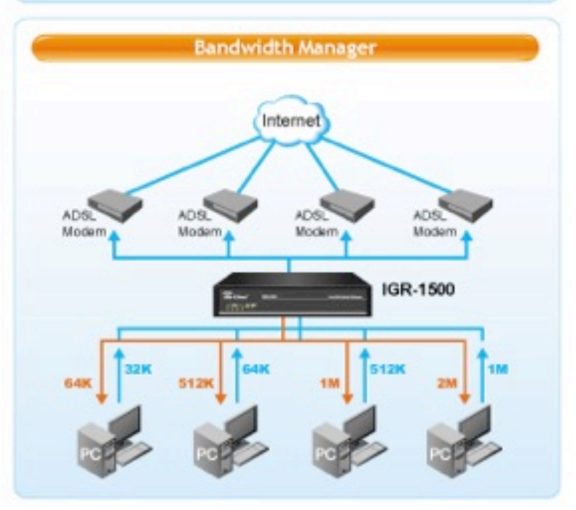


Imagen 6.14 (Casos de balanceo)

En nuestro caso nos interesa comprender el último de los cuatro, referido a la administración del ancho de banda.

En general en grandes redes, encontraremos en su casi mayoría, dos líneas de productos: **F5 Networks** y **Cisco ACE**.

a) F5 Networks *(de su propia Web http://www.f5.com):*

Model	***Advertised throughput***
- BIG-IP LTM	Virtual Edition 10 Mbit/s, 200 Mbit/s or 1 Gbit/s
- BIG-IP 1600	1 Gbit/s
- BIG-IP 3600	2 Gbit/s
- BIG-IP 3900	4 Gbit/s
- BIG-IP 6900	6 Gbit/s
- BIG-IP 8900	12 Gbit/s
- BIG-IP 8950	20 Gbit/s

- BIG-IP 11050 42 Gbit/s
- Viprion 2400 Up to 160 Gbit/s L4 & Up to 72 Gbit/s L7. Per Blade Up to 40G L4 & Up to 20G L7
- Viprion 4480 Up to 320 Gbit/s[15]

BIG-IP product modules:

- Local Traffic Manager (LTM): Local load balancing based on a full-proxy architecture.
- Global Traffic Manager (GTM): Global server load balancing using DNS.
- Link Controller: Inbound and outbound ISP load balancing.
- Application Security Manager (asM): A web application firewall.
- WebAccelerator: An asymmetric or symmetric advanced caching solution for HTTP and HTTPS traffic.
- Edge Gateway: An SSL VPN.
- WAN Optimisation Module: A data centre symmetric WAN optimization solution.
- Access Policy Manager (APM): Provides access control and authentication for HTTP and HTTPS applications.



Imagen 6.15 (F5 Viprion 4480)



Imagen 6.16 (F5 Viprion 4800)



Imagen 6.17 (F5 Viprion 4200 - Blade)

b) Cisco ACE: (ACE Application Control Engine)

Como veremos aquí abajo, estos balanceadores de Cisco, en realidad son módulos de hardware que se incorporan a diferentes productos de uso general como son determinadas familias de switch y routers, una vez incorporado este módulo, se gestiona como cualquier otro elemento de este fabricante

(de su propia Web: http://www.cisco.com/c/en/us/products/interfaces-modules/ace-application-control-engine-module/index.html)



Represent the state of the art in next-generation application switches for increasing the availability, performance, and security of data center applications.

The Cisco ACE family of application switches includes the Cisco ACE Service Module for the Cisco Catalyst 6500 Series Switches and Cisco 7600

Series Routers, as well as the Cisco ACE 4710 Appliance in a standalone form factor for discrete data center deployments.

Through a broad set of load balancing and content switching capabilities, coupled with unique virtualized architecture and granular user access control, Cisco ACE provides industry-leading time and cost reduction for application deployment, build-out, and performance or security enhancement. IT departments and end users benefit directly through faster application rollout, improved response time, and long-term investment protection.

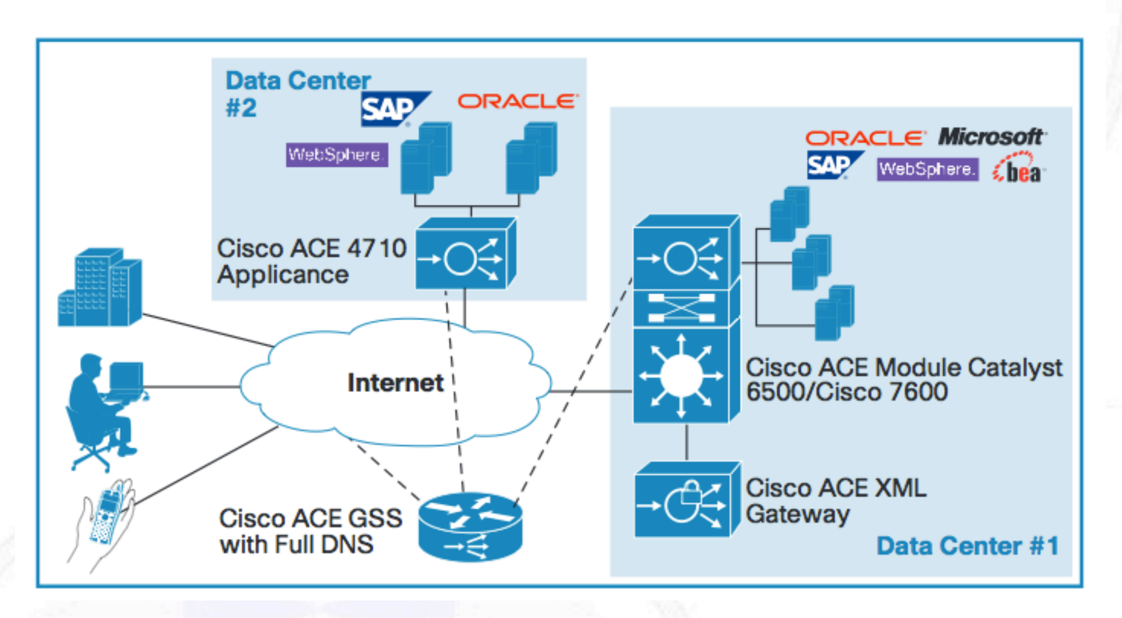


Imagen 6.18 (Opciones del despliegue Cisco ACE)



Imagen 6.19 (Modelos Cisco ACE)



Imagen 6.20 (Modelo Cisco ACE ampliado)

Una opción al alcance de todos es la implantación de un "**Linux Virtual Server**" (podemos ver el detalle en: http://www.linuxvirtualserver.org).

Esta nueva opción nos permite crear un cluster de servidores que realicen tareas de balanceo de carga sobre sistema operativo Linux. SI bien esta solución está diseñada específicamente para balanceo de carga y se ejecuta con el alto rendimiento que nos ofrece Linux, las capacidades finales de esta arquitectura tienen relación directa sobre el hardware que decidamos montarlo. Esta solución soporta balanceo de carga de alta disponibilidad sobre cualquier servicio de red (web, ftp, VoIP, multimedia, mail, etc).

Estos Virtual server se pueden implementar de tres formas

- Virtual Server vía NAT (VS/NAT): Permite balanceo de cargas entre servidores configurados con cualquier sistema operativo que soporte TCP/IP. Como necesita realizar la operación de NAT, esto implica una importante consumo de recursos.
- Virtual Server vía IP Tunneling (VS/TUN): Este balanceo puede ser empleado para alto rendimiento empleando "IP Tunneling", no necesita realizar operaciones sobre los paquetes, conmutando cada uno de ellos al destino final, basado únicamente en la lógica de balanceo.
- Virtual Server vía Direct Routing (VS/DR): Este balanceo es similar al anterior, pero no requiere el empleo de "IP tunneling", con lo cual la redirección de paquetes se realiza a través de interfaces físicas, lo que implica que debe existir una interfaz física por servidor.

Cada uno de ellso presenta una serie de ventajas y desventajas:

	VS/NAT	VS/TUN	VS/DR
server	any	tunneling	non-arp device
server network	private	LAN/WAN	LAN

server number	Low (10~20)	high	high
server gateway	load balancer	own router	own router

Como hemos mencionado, este servicio es un importante objetivo para cualquier intruso, por lo tanto es importante analizarlas para verificar su nivel de seguridad.

Dentro de la distribución de "**Kali**", encontramos un programa dentro del menú:

"**Application**" —> Kali Linux —> Information Gathering —> IDS/IPS Identification —> **lbd** (*Load Balancing Detector*).

Que nos permite analizar balanceo de carga sobre arquitecturas de DNS y Web.

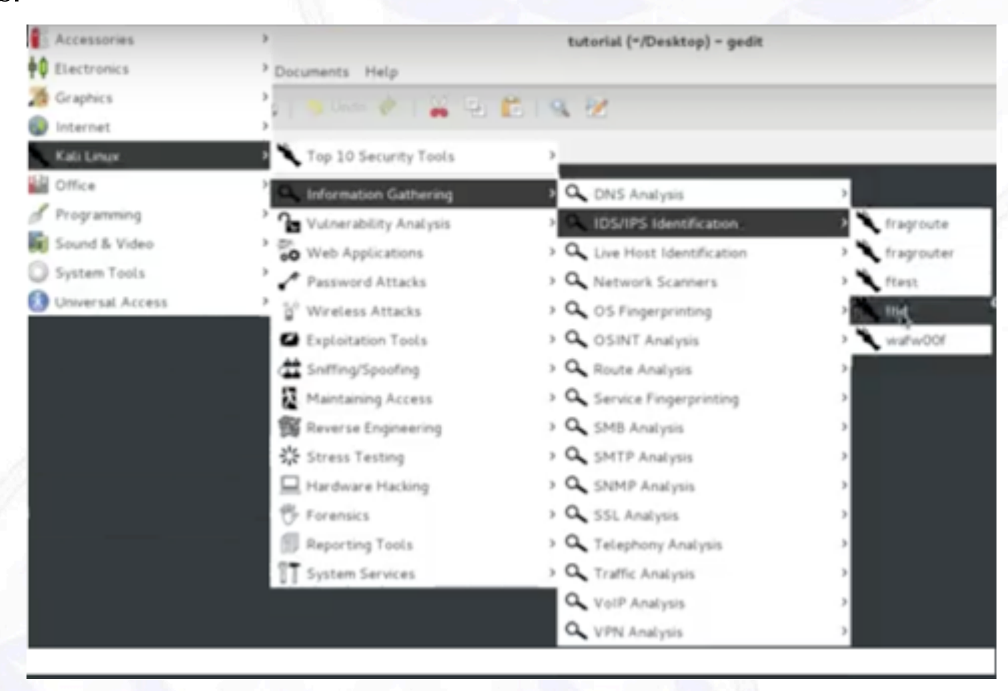


Imagen 6.21 (dentro de "Kali", software Load Balancing Detector)

La otra herrmienta que también posee Kali está dentro del menú: "Application" —> Kali Linux —> Web Application —> Web Vulnerability Scanner —> **w3af**

Esta aplicación posee un plugin denominado "**halberd**" que nos puede ser muy útil para evaluar balanceo de cargas frente a servidores Web

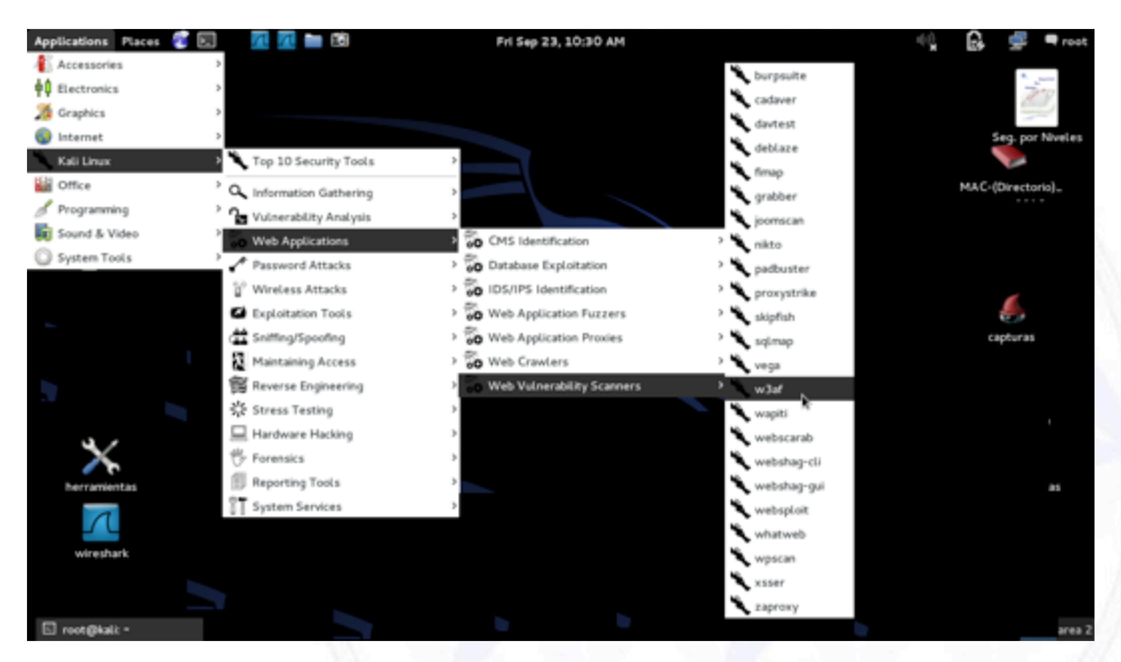


Imagen 6.22 (herramientas de "Kali")

6.8. Plataformas de sincronización de tiempo.

Este tema que, como hemos mencionado parece poco relevante, lo es en realidad y se convierte en vital a la hora de realizar cualquier análisis forense o intentar realizar cualquier seguimiento de actividad. Ya nos ha sucedido en reiteradas oportunidades que ante un incidencia determinada que abarca más de un nodo, a la hora de estudiarla, todo el trabajo se complica (*y mucho*) cuando no es posible seguir una base de tiempo común, pues comienzan a aparecer eventos que cronológicamente no coinciden y se debe realizar un alto esfuerzo adicional para encontrarle la lógica.

Mucho más grave que ello, es a su vez si se debe presentar pruebas legales ante cualquier incidencia, pues un fallo horario, es una realidad que puede tirar por tierra cualquier prueba o peritaje judicial.

El trabajo de sincronización de tiempos es sumamente sencillo y no requiere grandes inversiones materiales ni humanas, sencillamente es una cuestión procedimental y organizativa, en base a lo que propone el protocolo "**ntp**" (Network Time Protocol), es decir organizar una estructura jerárquica adecuada sobre la base de los "estratos ntp", y apuntar TODOS los nodos hacia el servidor ntp que le corresponda, nada más. Como medida de seguridad a evaluar, está que se configure la versión 3 o 4 de este protocolo que son las que ofrecen opciones de autenticación, justamente para evitar que cualquier intruso pueda modificar o forzar cualquier cambio horario.

Como referencia para cualquier implementación que realicemos sobre ntp, el mayor referente o nuestro punto de partida debería ser el **IETF NTP Working Group**:

http://support.ntp.org/bin/view/IETF/WebHome

Si nuestra organización desea tomar como referencia algún servidor de tiempo internacional, en este mismo grupo de trabajo podemos encontrar el listado por país:

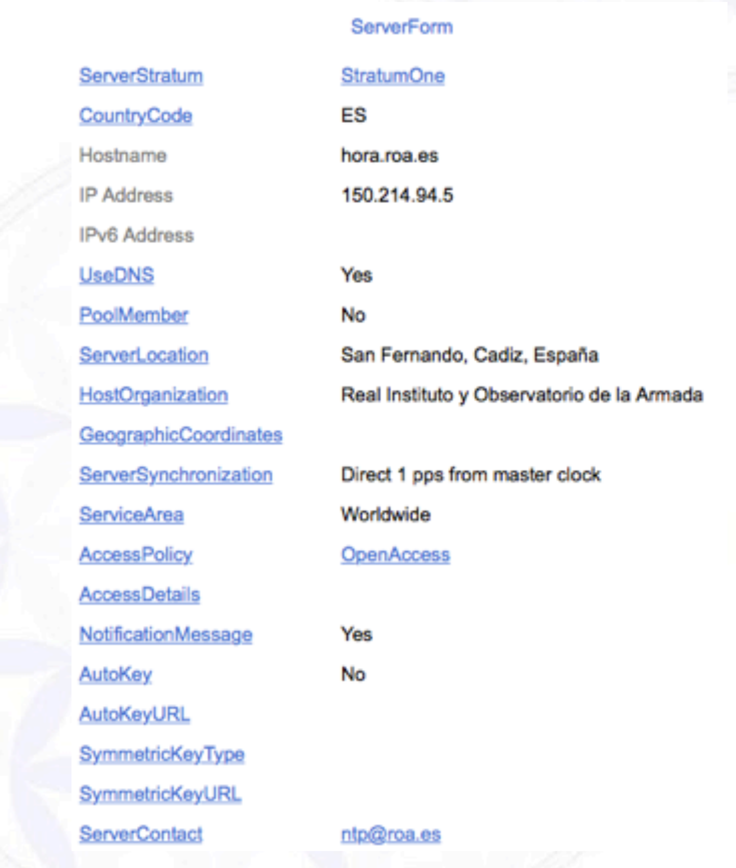
http://support.ntp.org/bin/view/Servers/StratumOneTimeServers

En el caso de España presentamos a continuación los que figuran disponibles:

ISO:	Location:	Host / Sponsor:	Service Area:	Access Policy:	Notify?	LastModified:
ES	San Fernando, Cadiz, España	Real Instituto y Observatorio de la Armada	Worldwide	OpenAccess	Yes	2016-02-02T07:44:58Z
ES	Laboratory of I2T Research Group, Faculty of Engineering, University of the Basque Country UPV/EHU, Bilbao, Basque Country, Spain.	I2T Research Group	Internet	OpenAccess	No	2015-06-12T14:26:53Z
ES	San Fernando, Cadiz, España	Real Instituto y Observatorio de la Armada	Worldwide	OpenAccess	Yes	2016-02-02T07:45:28Z

Imagen 6.23 (Servidores de tiempo disponibles en España)

Si seleccionamos, por ejemplo el primero de ellos, nos presenta la siguiente información:



ServerForm	
ServerStratum	StratumOne
CountryCode	ES
Hostname	hora.roa.es
IP Address	150.214.94.5
IPv6 Address	
UseDNS	Yes
PoolMember	No
ServerLocation	San Fernando, Cadiz, España
HostOrganization	Real Instituto y Observatorio de la Armada
GeographicCoordinates	
ServerSynchronization	Direct 1 pps from master clock
ServiceArea	Worldwide
AccessPolicy	OpenAccess
AccessDetails	
NotificationMessage	Yes
AutoKey	No
AutoKeyURL	
SymmetricKeyType	
SymmetricKeyURL	
ServerContact	ntp@roa.es

Image 6.24 (detalles del servidor: hora.roa.es)

El mensaje más importante a considerar es que su política de acceso es "Open Access", lo que nos indica que cualquier cliente puede hacer uso de su servicio de tiempo, siempre y cuando cumpla con unos pocos aspectos que se detallan en una guía en esta misma Web. Esto implica que podemos adoptarlo como "Strato 1" para nuestra empresa. Como se puede apreciar también, se declara como "StratumOne", esto implica que él a su vez está sincronizado con un nivel superior que será su "estato 0"

Si deseamos organizar nuestra jerarquía ntp dentro de la propia organización, por ejemplo, podemos adoptar este servidor de "**hora.roa.es**" como el "**estrato 1**", que será la "raíz" de toda la empresa, hacia él apuntar todos los routers de Core, que serán nuestro "**estrato 2**" y si deseamos seguir esta lógica, por ejemplo, cada área de la organización (TI, Red, Marketing, Ventas, etc.), empresas, clientes, parnters; pueden apuntar sus principales elementos hacia estos, conformando éste el "**estrato 3**" y con el criterio que cada área desee puede configurar sus propios "**estratos 4 o 5…**".

6.9. Plataformas de Autenticación y Control de Accesos.

Este tipo de plataformas son las que nos permiten regular y llevar el control sobre la metodología de validación y acceso de usuarios al segmento de red que deseemos. En cualquier red hoy en día, es normal que los diferentes operadores, partners, empleados o clientes deban acceder a sus dispositivos desde diferentes lugares físicos de trabajo. La primera opción que tenemos a mano es implementar una "máquina de salto", este tema lo desarrollaremos en el punto siguiente, pero los fabricantes ofrecen en la actualidad varios productos que son específicamente diseñados para esta actividad.

En realidad la principal ventaja que ofrece este tipo de plataformas es la posibilidad de crear VPNs y a su vez de operar en modo gráfico sobre el destino final, llevando todo el control estricto de la sesión.

Algunos de estos productos presentaremos a continuación.

6.9.1. Cisco Secure Access Control System.

Todo el detalle de esta familia de productos podemos verlo en http://www.cisco.com.

Cisco ACS se presenta como un complemento más de su solución que este fabricante llama "TrustSec". Provee servicio de TACACS+ y RADIUS, cualquier tipo de políticas de acceso y cumplimiento legal, permitiendo también acceso vía VPN.

Cisco introduce dos nuevos conceptos con esta familia de dispositivos:

- Política de punto de administración (PAP)

- Política de punto de decisión (PDP)

Que incluyen:

- Única, flexible, y detallada administración de dispositivo en redes IPv4 e IPv6, con capacidades de auditoría y de reportes que se requieran para el cumplimiento legal.
- Un potente modelo de políticas basado en reglas y atributos que aborda de manera flexible las necesidades de direccionamiento basado en reglas complejas.
- Una interfaz gráfica de usuario basada en interfaz Web con navegación intuitiva y flujo de trabajo accesible desde ambos clientes IPv4 e IPv6.
- Monitorización avanzado e integrada, reportes y capacidades de resolución de problemas para un excelente control y visibilidad.
- Integración con políticas de bases de datos e identidades externas, incluyendo Microsoft Active Directory y Lightweight Directory Access Protocol (LDAP), que simplifica la configuración de políticas y de mantenimiento.
- Un modelo de implementación distribuida que soporta despliegues a gran escala y proporciona una solución de alta disponibilidad.



imagen 6.25 (Secure Network Server 3415 for Access Control System 5.8)

Un producto que es importante también emplear con este tipo de plataformas es el "VPN Client" que se trata de un software que se instala en el dispositivo cliente y nos permite conectarnos a la red destino creando una VPN (cifrada) a través de Internet. Con el empleo de este software, al realizar esta conexión segura, se nos asigna una dirección IP destino dentro del rango de la red final, por lo tanto terminamos operando exactamente igual que si estuviéramos conectados de forma directa a esa LAN.

A continuación presentamos una imagen de este cliente.

imagen 6.26 (Cliente Cisco VPN)

En la imagen anterior, hemos desplegado las tres ventanas que nos ofrece este cliente VPN para que podamos apreciar todas las opciones de seguridad que contempla.

6.9.2. Citrix Access Gateway VPX.



Para ver el detalle del producto podemos ir a: https://www.citrix.es/products/.

Si bien Citrix ofrece opciones de hardware, lo más novedoso es este nuevo producto (Citrix Access Gateway VPX) que ofrece hoy un entorno virtual. Se trata de un software para virtualizar servidores, aplicaciones y entornos de escritorio. Se puede

instalar sobre el propio hardware y para el acceso, los clientes puede emplear Citrix online plug-ins y conectarse a Citrix XenAppTM o a Citrix XenDesktop Server.

Los usuarios pueden ser validados contra varios sistemas de autenticación con el objetivo de proteger aplicaciones seguras y datos. El dispositivo final realiza un escaneo de seguridad sobre los dispositivos cliente y determina la validez de la configuración de seguridad que se haya decidido. Para los clientes que no superen el análisis de seguridad, se proporciona remediación poniéndolos en cuarentena (el tiempo que se haya configurado) para el cumplimiento de las políticas de seguridad de la organización.

Nuevamente una opción desde el lado cliente es hacer uso de la versión "cliente" de software, una imagen de esta presentamos a continuación.

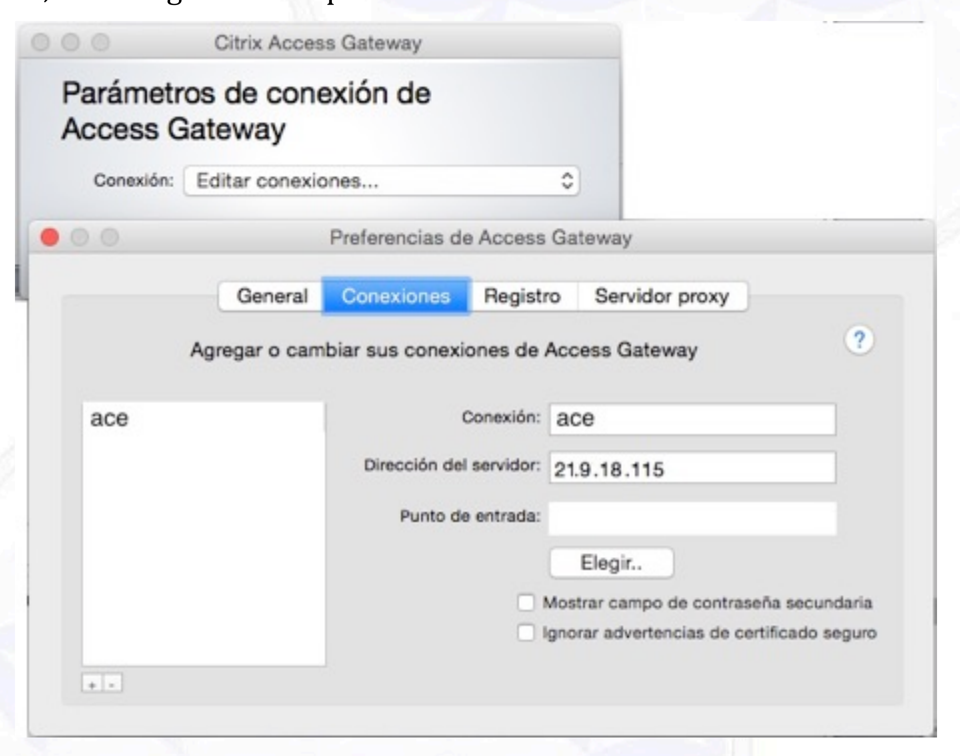


imagen 6.27 (Cliente Citrix VPN)

6.9.3. Fortinet.



Podemos ver todo el detalle en: https://www.fortinet.com

Fortinet es otra empresa líder del mercado de seguridad, ofrece una gama completa de soluciones para todo tipo de medidas de seguridad que deseemos aplicar en nuestras redes, aquí abajo presentamos una imagen que hemos extraído de su Web, en la URL:

https://www.fortinet.com/solutions/small-business/secure-communications.html

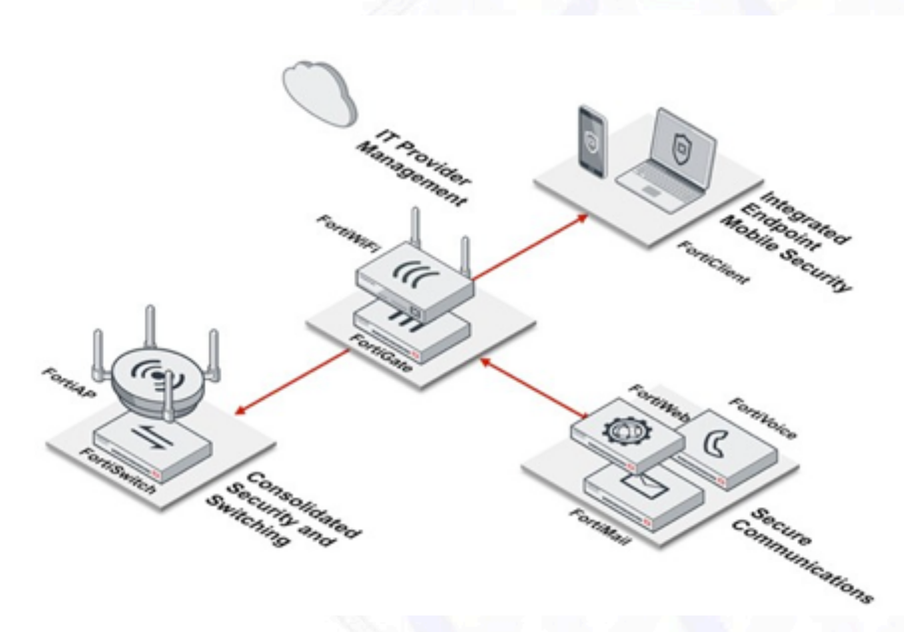


Imagen 6.28 (arquitectura de seguridad Fortinet para pequeñas empresas)

La imagen anterior describe resumidamente el conjunto de productos para cualquier pequeña empresa, los cuáles pueden ser escalados hasta la magnitud que se desee.

Sería muy difícil poder resumir toda la gama de soluciones de acceso y seguridad que ofrece este fabricante, pues gran parte de sus productos integran funcionalidades de autenticación y control de accesos, por esa razón a continuación presentamos algunas de sus soluciones, desde las grandes empresas hasta la pequeña.



Imagen 6.29 (The FortiGate NGFW 1000 - 7000 High-End series)



Imagen 6.30 (The FortiGate NGFW 900 - 100 mid-range series)



Imagen 6.31 (FortiGate NGFW 90 - 30 series appliances)



Imagen 6.32 (Fortinet Secure Network Authentication)

6.9.4. NAKINA.



NAKINA es tal vez uno de los despliegues más avanzados como plataforma de seguridad en cuanto a: Autenticación, control de accesos, segmentación e inventario. Ofrece todo una gama de soluciones, que podemos resumir en la siguiente imagen.

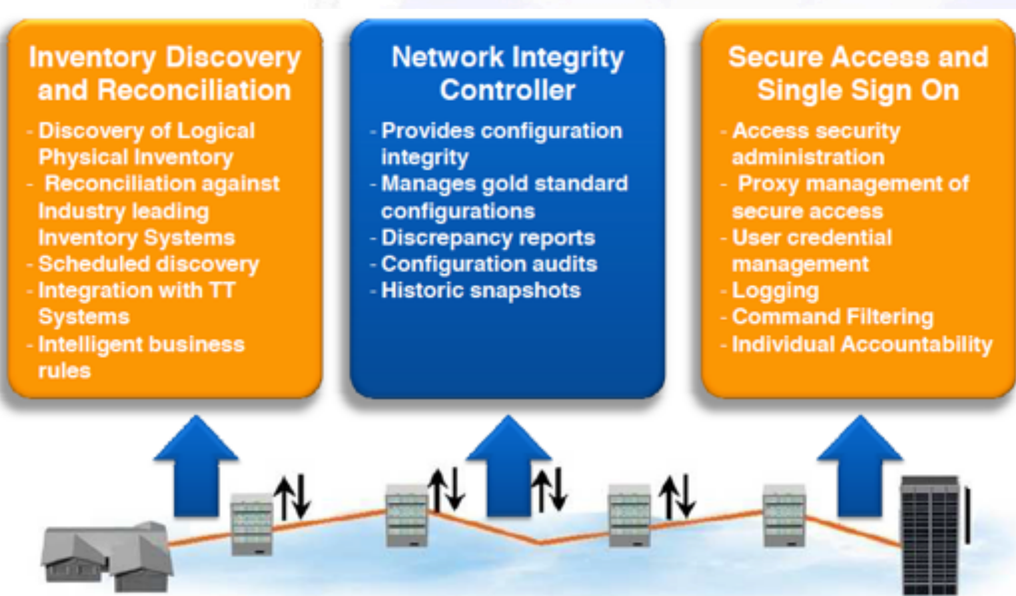


Imagen 6.33 (Soluciones que ofrece NAKINA)

En cuanto a control de accesos remotos la imagen que sigue nos presenta gráficamente cómo es la solución.

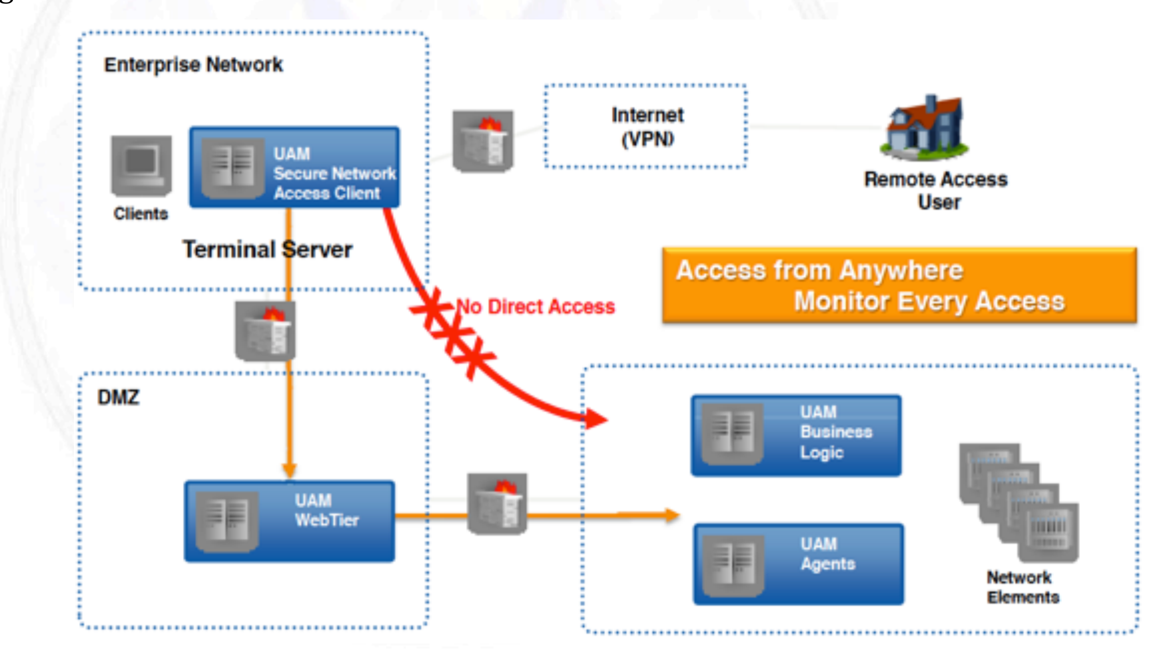


Imagen 6.34 (Accesos VPN que ofrece NAKINA)

Por último, podemos ver que el cliente final tiene la capacidad de acceder a su propia máquina de escritorio dentro de la empresa y trabajar de forma remota sobre ella.

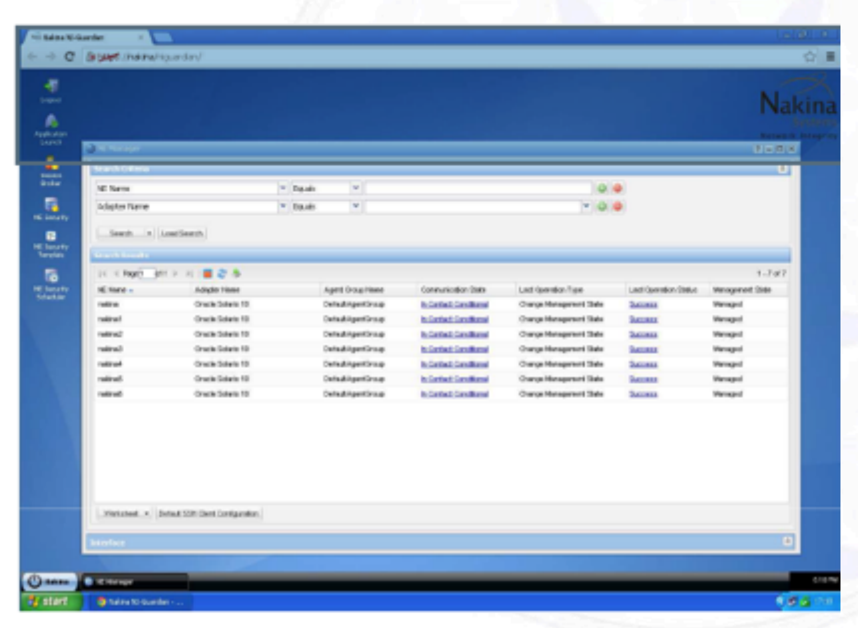


Imagen 6.35 (Escritorio remoto cliente con acceso vía NAKINA)

Resumidamente, las ventajas que ofrece este fabricante son:

- Login individual para cada usuario, regulado por destino y aplicación.
- Elimina la posibilidad de contraseñas compartidas.
- Provee auditoría y video logging de la actividad de los usuarios de forma individual (*Esta característica de "video" sobre sesiones gráficas lo posiciona prácticamente como único en el mercado*).
- Provee capacidad de gestión global de credenciales.
- Incrementa el control de los permisos de acceso con mayor granularidad y definición de roles.
- Aplica verdaderamente el concepto de "Single Sign On".
- Seguridad proactiva y auditoría de parámetros y acciones.
- Ofrece la opción de "Inventario activo" de red.

Si bien existen varios productos más en el mercado para configurar infraestructras de control de accesos, en esta sección hemos querido presentar sólo algunos de ellos, con la intención de destacar su importancia y que el lector pueda conocer las características básicas de cada uno de ellos. Por supuesto a la hora de

adoptar una decisión sobre esta actividad en nuestra red, sería importante profundizar más sobre la oferta del mercado.

Controles de evasión de autenticación

Hemos verificado que en muchos casos, por más que existan plataformas de autenticación, metodologías y mecanismos para ello, la rutina, comodidad y/o resistencia al cambio hacen que los administradores continúen empleando cotidianamente este tipo de cuentas de "emergencia" (genéricas o locales) que por razones de disponibilidad es necesario dejar habilitadas. Cuando esto sucede, es realmente un problema, pues en definitiva se está tirando por tierra todos los mecanismos implementados para "trazabilidad".

La forma más práctica de verificar esta mala práctica, es a través del análisis de Logs, pues en ellos queda registrado (*si están debidamente configurados….. que es como debería ser*) al menos todo acceso y cierre de sesión, por lo tanto, nuestra tarea en este punto es acceder o solicitar una consulta a estos Logs, y también guardar los mismos para un análisis posterior.

A continuación vamos a presentar un caso real que hemos encontrado en una red, que nos demuestra que los mismos no son explotados adecuadamente y no nos sirven en estos casos para generar las alarmas correspondientes de intentos "peligrosos" de autenticación.

Ejemplo: (Uno de los puntos de nuestro Diagnósticos de seguridad a una red)

No es motivo de esta parte del texto ahondar en aspectos de detalle sobre el análisis de Logs, pero de la breve evaluación de uno sólo de los archivos recibidos de los Logs de una herramienta de Gestión de firewall (En este caso "Firemon"), en una red veamos que se puede apreciar lo siguiente:

***71309**;30Oct2012;16:13:43;10.116.246.97;log;accept;;;outbound;CPMI Client;;;;LogIn;;na0078;firemon.xxxxxxxx;;; **Administrator Login;Failure**; Administrator failed to log in: Unknown **administrator** na0078;11;; ;;10.116.246.112;Network*
………
…..
***71609**;31Oct2012;5:57:43;10.116.246.97;log;accept;;;outbound;CPMI Client;;;;Log In;;na0078; firemon.xxxxxxxx;;;**Administrator Login;Failure**;Administrator failed to log in: Unknown **administrator** na0078;11;;;;10.116.246.112;Network*
……..
……
***76883**;9Nov2012;16:47:45;10.116.246.97;log;accept;;;outbound;CPMI Client;;;;Log In;;na0078; firemon.xxxxxxxx;;; **Administrator Login;Failure**;Administrator failed to log in: Unknown **administrator** na0078;11;;;;10.116.246.112;Network*

………
76889*;9Nov2012;17:05:55;10.116.246.97;log;accept;;;outbound;CPMI Client;;;;Log In;;na0078; firemon.xxxxxxxx;;;* ***Administrator Login;Failure****;Administrator failed to log in: Unknown* ***administrator*** *na0078;11;;;;10.116.246.112;Network*
…………
……
86887*;27Nov2012;10:54:57;10.116.246.97;log;accept;;;outbound;CPMI Client;;;;Log In;;na0078; firemon.xxxxxxxx;;;* ***Administrator Login;Failure****;Administrator failed to log in: Unknown* ***administrator*** *na0078;11;;;;10.116.246.112;Network*

*Entre el primero (**71309**) y el último (**86887**), se han generado casi unos 5000 eventos de **login failed** con la cuenta "**Administrator**" (son más de 700 páginas sólo de este Log, y al menos **un mes generándolo**….. no podemos afirmar que hayan sido más pues ese día comienzan los registros que hemos recibido). No podemos saber si se trató de un ataque o una cuenta automatizada (sería muy difícil poder justificar este empleo por parte de empleados de la empresa xxxxxxxxx sobre un FW….), tampoco podemos saber si el último Log (**86887**) se debió a que se solucionó el tema por parte de los administradores de esta red,…… o este usuario (o tal vez intruso) logró el acceso y la autenticación que buscaba.*

*Lo que sí se puede afirmar de forma rotunda es que estos Logs no generaron ningún tipo de alarma (o no hubo nadie que la miró) y que durante todo este tiempo nadie analizó los logs, pues se trata de una evento CRÍTICO que está alertando de una actividad altísimamente sospechosa, ejecutada con la cuenta de máximo privilegio sobre la plataforma que nos abriría las puertas a **TODA** la infraestructura de esta red, hasta donde se desee llegar si se obtuviera este acceso…….* ***¿Se obtuvo….., o se solucionó???***

Ejemplo 2: (análisis de Logs de otra red)

```
7|Jun 18 2012|16:32:24|715046|||||Group = vpn_sol, Username = elen.cm, IP = 10.1.1.1, constructing qm hash payload
7|Jun 18 2012|16:32:24|715046|||||Group = vpn_sol, Username = elen.cm, IP = 10.1.1.1, constructing blank hash payload
7|Jun 18 2012|16:32:24|715036|||||Group = vpn_sol, Username = elen.cm, IP = 10.1.1.1, Sending keep-alive of type DPD R-U-THERE-ACK (seq number
.......
7|Jun 18 2012|16:32:24|715046|||||Group = vpn_nc, Username = alan.unoz, IP = 10.1.20.17.4, constructing qm hash payload
7|Jun 18 2012|16:32:24|715046|||||Group = vpn_nc, Username = alan.unoz, IP = 10.1.20.17.4, constructing blank hash payload
7|Jun 18 2012|16:32:24|715036|||||Group = vpn_nc, Username = alan.unoz, IP = 10.1.20.17.4, Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x8c13cecd
......
```

```
7|Jun 18 2012|16:32:24|715046|||||Group = vpn_especial, Username = JCar, IP = 2.246.65.235, constructing qm hash payload
7|Jun 18 2012|16:32:24|715046|||||Group = vpn_especial, Username = JCar, IP = 2.246.65.235, constructing blank hash payload
........
7|Jun 18 2012|16:32:34|716047|||||Group = vpn_admin, Username = admin, IP = 192.168.10.2, cmd enable
7|Jun 18 2012|16:39:34|716049|||||Group = vpn_admin, Username = admin, IP = 192.168.10.2, cmd ifconfig
7|Jun 18 2012|16:32:54|716053|||||Group = vpn_admin, Username = admin, IP = 192.168.10.2, cmd Gi 0/1/1
........
6|Jun 18 2012|16:32:23|109025|10.184.67.159|63999|10.232.50.38|53| Authorization denied (acl=#ACSACL#-IP-D_hp16-4a) for user 'e.lpd' from 10.184.67.159/63999 to 10.232.50.38/53 on interface externa using UDP
6|Jun 18 2012|16:32:23|109025|10.184.67.163|137|10.184.67.255|137| Authorization denied (acl=#ACSACL#-IP-D_A_10_157-4e) for user 'e.fbes' from 10.184.67.163/137 to 10.184.67.255/137 on interface externa using UDP
......
6|Jun 18 2012|16:32:23|109025|10.184.67.165|137|10.184.67.255|137| Authorization denied (acl=#ACSACL#-IP-C_Res5-474) for user 'e10.jrr' from 10.184.67.165/137 to 10.184.67.255/137 on interface externa using UDP
........
6|Jun 18 2012|16:32:23|109025|10.184.67.148|1465|172.16.100.112|53| Authorization denied (acl=#ACSACL#-IP-A_IR-AC-40c) for user 'e26.rmla' from 10.184.67.148/1465 to 172.16.100.112/53 on interface externa using UDP

6|Jun 18 2012|16:32:23|109025|10.184.67.148|1465|10.232.50.38|53| Authorization denied (acl=#ACSACL#-IP-DACL_I-C-4ecc52) for user 'e26.rmla' from 10.184.67.148/1465 to 10.232.50.38/53 on interface externa using UDP
```

En la captura anterior, hemos querido poner de manifiesto un hecho al cual invitamos al lector de intentar encontrar , antes de seguir adelante con el párrafo siguiente.

Los Logs que se presentaron, fueron los generados por un servidor de autenticación y control de acceso, los cuáles como hemos mencionado, tienen toda la capacidad de realizar el seguimiento de la actividad de usuarios, generar alarmas y reportes altamente personalizados. En este caso, estos Logs no generaban ningún tipo de alarmas, ni se analizaban. Hemos reducido el volumen de los mismos en este texto, pero si prestamos atención, hay un usuario "**admin**" que se está validando correctamente y ejecutando comandos (`cmd enable, cmd ifconfig`) sobre un dispositivo (`192.168.10.2`). Por el tipo de comando, se trata de un router Cisco, que escaló privilegios (con la cuenta "admin"), está por realizar actividades de configuración sobre una interface, y por si esto fuera poco, en un horario de alta actividad

(|16:32:34| horas). Si alguien observara estos Logs, o hubiese preparado este servidor para que genere alarmas o reportes adecuados, no hay duda que debería haber informado que:

- esta cuenta "admin" está habilitada en ese router.
- esta cuenta "admin" puede entrar en modo privilegiado.
- Este usuario "admin" esta ejecutando comandos de configuración.
- Lo hace fuera de ventana (es decir, estas actividades de gestión JAMÁS deben realizarse en horarios pico, sino que se deben realizar en "ventanas de tiempo" nocturnas o de baja actividad, en las cuáles cualquier fallo impactaría menos la red).

6.10. Herramientas de gestión de Routers.

Si bien hemos mencionado que este tipo de dispositivos, en general suelen gestionarse a través de línea de comandos, y lo normal es que cualquier operador cualificado conozca esta metodología, en el mercado también existen herramientas que ayudan o complementan esta tarea. Este tipo de herramientas, nos ofrecen la ventaja que "centralizan" los accesos a la totalidad de los router de la empresa y por ejemplo podemos ejecutar actualizaciones o modificaciones de forma masiva, manteniendo la versión anterior en "segundo plano" para restaurarla inmediatamente ante fallos, realizan de forma robusta toda la política de resguardo y recuperación que deseemos implantar, permiten también monitorizar parámetros (como hemos hecho con nuestros scripts en bash) para evaluar el estado de configuración de los routers, y también una gestión de inventario activa, pues tiene permanente conocimiento de la arquitectura de la red.

Cada fabricante ofrece sus herramientas propietarias, por ejemplo:

- Cisco Works.
- Juniper Network Management.
- U-2000 o M-2000 de Huawei.
- OSS-RC de Ericsson
- Voyager de Nokia.
- Etc..

Pero también existen fabricantes específicos que soportan todo tipo de productos. Presentamos a continuación una de ellas, que hemos visto como eficiente para este tipo de actividades, en los ejemplos que siguen esta tarea fue ejecutada con la herramienta "Net Doctor" de "**OPNET**" y veremos varias imágenes capturadas de informes que se generan con esta herramienta de gestión de reglas de router, no para

hacer publicidad a un fabricante en concreto, sino para que podamos apreciar la variedad de información que dese el punto de vista de la seguridad nos pueden ofrecer.

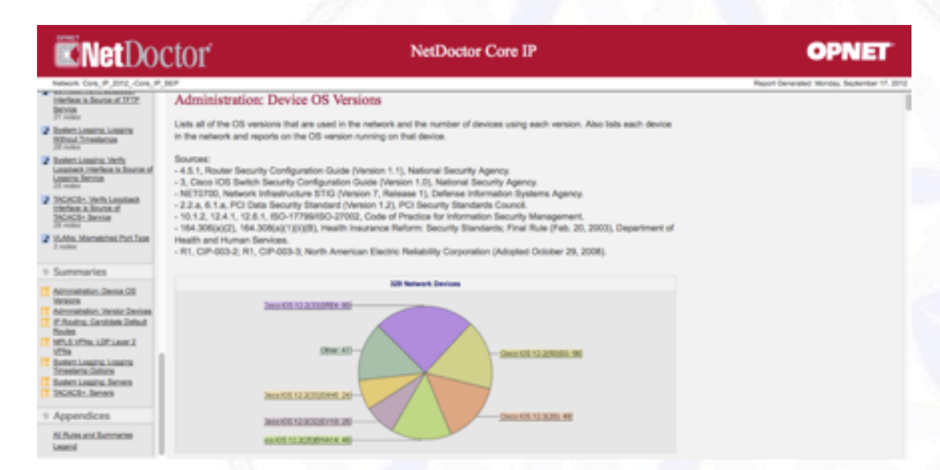


Imagen 6.36 (Herramienta NetDoctor de OPNET – Versiones OS)



Imagen 6.37 (Herramienta NetDoctor de OPNET – MPLS y VPNs)

En la imagen anterior podemos ver cómo nos ofrece información sobre las VPNs que tengamos configurada en nuestra red y su relación con MPLS.

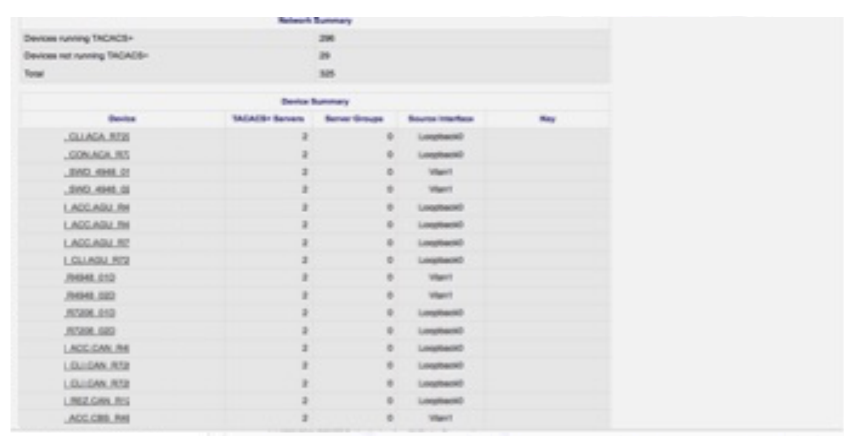


Imagen 6.38 (Herramienta NetDoctor de OPNET – TACACS+)

En la anterior imagen, se puede ver cómo evalúa la configuración de TACACS+ en los routers que tiene dados de alta, cuáles de ellos cumplen, cuáles no y luego el listado de las interfaces por las que se puede acceder a los mismos.

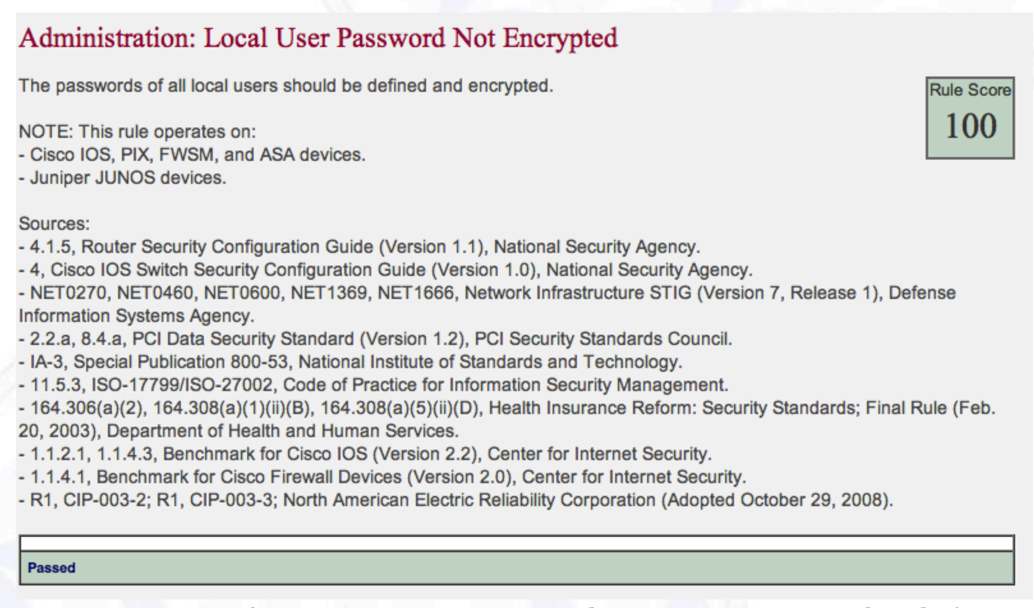


Imagen 6.39 (Herramienta NetDoctor de OPNET – usuarios locales)

En la imagen anterior podemos ver que la totalidad de estos routers cumplen (Rule Score 100) con no emplear usuarios locales sin criptografía robusta.

Administration: Verify Timeout for Login Sessions

This rule verifies that a timeout value is specified for login sessions so that the device automatically logs out a user session if it becomes idle.

Rule Score
100

NOTE: This rule operates on:
- Cisco IOS, PIX, FWSM, and ASA devices
- Juniper JUNOS devices.

Sources:
- 4.1.5, Router Security Configuration Guide (Version 1.1), National Security Agency.
- 5, Cisco IOS Switch Security Configuration Guide (Version 1.0), National Security Agency.
- NET1381, NET1390, NET1624, NET1639, NET1645, Network Infrastructure STIG (Version 7, Release 1), Defense Information Systems Agency.
- 2.2.a, 8.5.15, PCI Data Security Standard (Version 1.2), PCI Security Standards Council.
- AC-12, Special Publication 800-53, National Institute of Standards and Technology.
- 11.5.1, 11.5.5, ISO-17799/ISO-27002, Code of Practice for Information Security Management.
- 164.306(a)(2), 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(C), 164.312(a)(2)(iii), Health Insurance Reform: Security Standards; Final Rule (Feb. 20, 2003), Department of Health and Human Services.
- 1.1.2.4, Benchmark for Cisco IOS (Version 2.2), Center for Internet Security.
- 1.1.2.5, Benchmark for Cisco Firewall Devices (Version 2.0), Center for Internet Security.
- R1, CIP-003-2; R1, CIP-003-3; North American Electric Reliability Corporation (Adopted October 29, 2008).

Passed

Imagen 6.40 (Herramienta NetDoctor de OPNET –Time Out Logoff)

Todas las sesiones tienen configurado el Time Out correspondiente.

System Logging: Verify Syslog Trap Severity

This rule verifies that log messages of the specified level are logged.

Rule Score
100

NOTE:
This rule operates on:
- Cisco IOS, PIX, FWSM, and ASA devices.
- Juniper JUNOS devices.

Sources:
- 3.3.3, 4.5.2, Router Security Configuration Guide (Version 1.1), National Security Agency.
- 12, Cisco IOS Switch Security Configuration Guide (Version 1.0), National Security Agency.
- NET1021, Network Infrastructure STIG (Version 7, Release 1), Defense Information Systems Agency.
- 2.2.a, PCI Data Security Standard (Version 1.2), PCI Security Standards Council.
- AU-3, IR-5, SI-7, Special Publication 800-53, National Institute of Standards and Technology.
- 10.6.1, 10.10.1, 10.10.2, 10.10.5, ISO-17799/ISO-27002, Code of Practice for Information Security Management.
- 164.308(a)(5)(ii)(C), Health Insurance Reform: Security Standards; Final Rule (Feb. 20, 2003), Department of Health and Human Services.
- 1.2.3.5, Benchmark for Cisco IOS (Version 2.2), Center for Internet Security.
- 1.2.3.6, Benchmark for Cisco Firewall Devices (Version 2.0), Center for Internet Security.
- R1, CIP-003-2; R1, CIP-003-3; R3, CIP-005-2; R3, CIP-005-3; R6.3, CIP-007-2a; R6.3, CIP-007-3; North American Electric Reliability Corporation (Adopted October 29, 2008).

Passed

Imagen 6.41 (Herramienta NetDoctor de OPNET – Syslog)

AAA: Accounting References Undefined TACACS+ Method

If TACACS+ is used as an accounting method, then the device should be configured to communicate with at least one TACACS+ server. Otherwise, the TACACS+ method will fail.

Rule Score
100

Sources:
- 13, Cisco IOS Switch Security Configuration Guide (Version 1.0), National Security Agency.
- 2.2.a, 10.2.2, PCI Data Security Standard (Version 1.2), PCI Security Standards Council.
- AC-13, IR-5, Special Publication 800-53, National Institute of Standards and Technology.
- 10.1.2, 10.1.3, 10.10.1, 10.10.2, 10.10.4, ISO-17799/ISO-27002, Code of Practice for Information Security Management.
- 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), Health Insurance Reform: Security Standards; Final Rule (Feb. 20, 2003), Department of Health and Human Services.
- R1, CIP-003-2; R1, CIP-003-3; R3, CIP-005-2; R3, CIP-005-3; R5, CIP-007-2a; R5, CIP-007-3; North American Electric Reliability Corporation (Adopted October 29, 2008).

Passed

Imagen 6.42 (Herramienta NetDoctor de OPNET – AAA)

No hemos querido insertar más imágenes para no extender más este punto, solamente dejar presentadas algunas de las opciones que este tipo de herramientas nos ofrecen para que el lector pueda considerarlas ala hora de adoptar decisiones de seguridad sobre su infraestructura de Routers.

6.11. Herramientas de gestión de Firewalls.

Hemos mencionado en la sección correspondiente a filtrado, que existen este tipo de herramientas haciendo referencia a tres de ellas que conocemos (Algosec, Tuffin, Firemon). En una gran red, deberíamos considerar seriamente el empleo de alguna herramienta de este tipo pues a medida que el volumen de reglas va creciendo, en general se termina transformando en imposible de garantizar su adecuado funcionamiento.

Este tipo de herramientas nos ofrecen opciones para la decisión de modificación, borrado o alta de nuevas reglas pues analizan las vigentes y nos informan si puede ser "optimizada" la que estamos por ingresar o modificar, o inclusive si es redundante. Llevan también el control de los "Hits" (es decir la cantidad de veces que ha aplicado cada una de las reglas) y sobre estos cálculos nos informan el "peso" que tiene cada regla para optimizar el rendimiento, controlan la seguridad perimetral, informándonos si estamos dejando brechas de seguridad, etc.

Para poder centrarnos únicamente en ofrecer una visión de la potencia de las mismas, hemos seleccionado una de ellas (no porque sea mejor o peor que el resto, sino sencillamente para presentar imágenes gráficas al lector), en los párrafos siguientes veremos las capacidades básicas que nos ofrece la herramienta FW Analyzer de Algosec.

Esta herramienta permite realizar un trabajo de análisis, seguimiento de reglas de FWs, optimización y reportes.

Se presentan a continuación algunos ejemplos del tipo de trabajo que podemos realizar:

a) "Peso en las reglas":

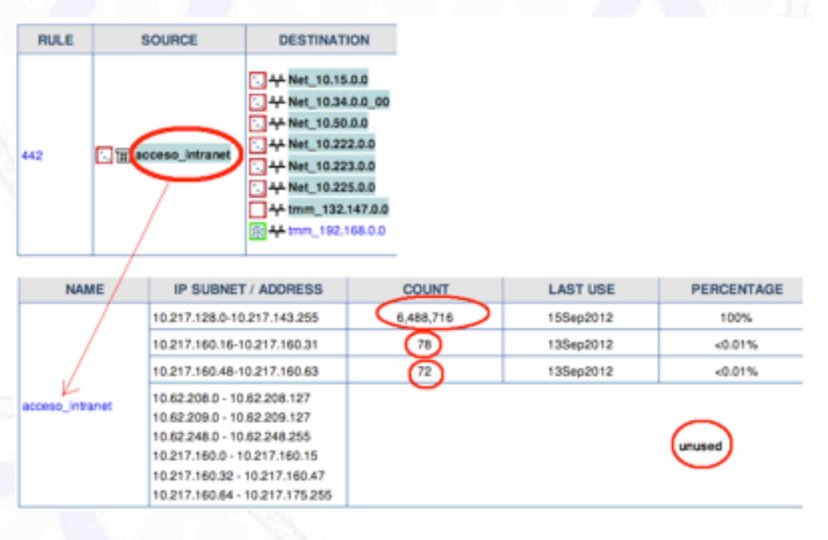
La toma de decisiones que adopta un FW es un proceso que se evalúa de forma secuencial, es decir por cada trama que le llega, analiza la regla Nº 1, dentro de ella comienza por la primera dirección IP (*o red*) de esa regla, compara su origen y/o destino, si los campos de la trama coinciden con alguno de ellos, cumple la condición (*básicamente: deny o permit*), si no coinciden, compara con la segunda dirección de la regla, la tercera, cuarta….. luego pasa a la segunda

regla repitiendo esta lógica hasta el final de las reglas (*si es que no se presenta ninguna coincidencia con lo determinado en cada renglón de cada una de las reglas*).

Entendiendo esta lógica, **es estrictamente natural, colocar en las primeras reglas** a aquellas que una herramienta como la de Algosec nos indica que son las que más frecuentemente se activan, pues <u>con ello evidentemente se están evitando cientos, miles y hasta millones de comparativas por cada trama</u> que le llega al dispositivo. La variación de la eficiencia de un FW realizando este trabajo es exponencial.

Abajo se presentan una serie de imágenes de los reportes de esta herramienta:

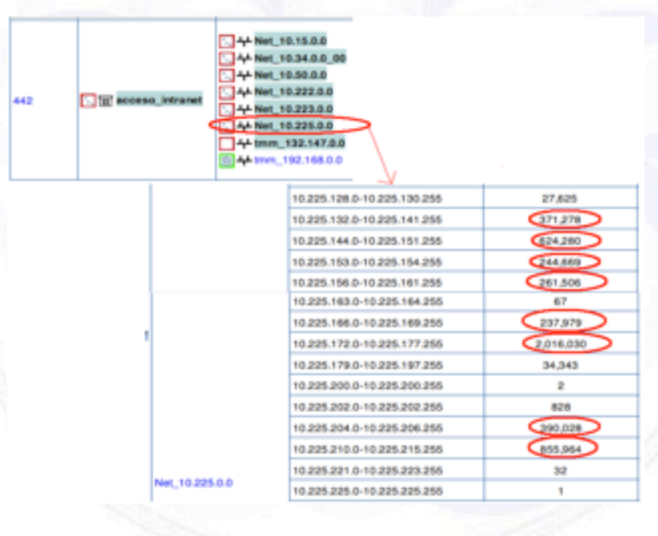
En esta primera imagen, se aprecia la regla Nº 442, donde el campo "Source" el objeto es "**acceso_Internet**". La flecha roja, indica el siguiente cuadro, donde se desglosan las redes que componen este "objeto".



RULE	SOURCE	DESTINATION
442	acceso_intranet	Net_10.15.0.0 Net_10.34.0.0_00 Net_10.50.0.0 Net_10.222.0.0 Net_10.223.0.0 Net_10.225.0.0 tmm_132.147.0.0 tmm_192.168.0.0

NAME	IP SUBNET / ADDRESS	COUNT	LAST USE	PERCENTAGE
acceso_intranet	10.217.128.0-10.217.143.255	6,488,716	15Sep2012	100%
	10.217.160.16-10.217.160.31	78	13Sep2012	<0.01%
	10.217.160.48-10.217.160.63	72	13Sep2012	<0.01%
	10.62.208.0 - 10.62.208.127 10.62.209.0 - 10.62.209.127 10.62.248.0 - 10.62.248.255 10.217.160.0 - 10.217.160.15 10.217.160.32 - 10.217.160.47 10.217.160.64 - 10.217.175.255			unused

Este es un buen ejemplo de algo que está bien, pues como se aprecia en el orden o secuencia de la misma, la primera de ellas tienen 6.488.716 ocurrencias o coincidencias con las tramas que ingresaron a este router, y las siguientes prácticamente nada.



442	acceso_intranet	Net_10.15.0.0 Net_10.34.0.0_00 Net_10.50.0.0 Net_10.222.0.0 Net_10.223.0.0 Net_10.225.0.0 tmm_132.147.0.0 tmm_192.168.0.0

Net_10.225.0.0	10.225.128.0-10.225.130.255	27,625
	10.225.132.0-10.225.141.255	371,278
	10.225.144.0-10.225.151.255	524,280
	10.225.153.0-10.225.154.255	244,669
	10.225.156.0-10.225.161.255	261,506
	10.225.163.0-10.225.164.255	67
	10.225.166.0-10.225.169.255	237,979
	10.225.172.0-10.225.177.255	2,016,030
	10.225.179.0-10.225.197.255	34,343
	10.225.200.0-10.225.200.255	2
	10.225.202.0-10.225.202.255	828
	10.225.204.0-10.225.206.255	390,028
	10.225.210.0-10.225.215.255	855,964
	10.225.221.0-10.225.223.255	32
	10.225.225.0-10.225.225.255	1

Sin embargo, en esta segunda imagen se aprecia que el objeto "**Destino**" (que son varios miles de direcciones IP), coinciden en más de 5.000.000 de ocurrencias con una de las últimas reglas (442), es decir que en estas 5.000.000 de ocurrencias recorrió inútilmente miles de direcciones IP previas correspondientes a las redes que están sobre esta.

NAME	IP SUBNET / ADDRESS	COUNT
Net_10.50.0.0	10.50.48.0-10.50.48.255	168
	10.50.93.0-10.50.93.255	1
	10.50.130.0-10.50.130.255	1
	10.50.181.0-10.50.181.255	1
	10.50.0.0 - 10.50.47.255 10.50.49.0 - 10.50.92.255 10.50.94.0 - 10.50.129.255 10.50.131.0 - 10.50.180.255 10.50.182.0 - 10.50.255.255	unused

Como último ejemplo pegamos a continuación (*siempre dentro de la regla 442 de los párrafos anteriores*) las ocurrencias de la primera de estas redes, la **10.50.0.0** (*se presenta en la primera de estas imágenes*) que como se puede apreciar son también varios cientos de direcciones IP y sólo posee 171 coincidencias. Millones y millones de tramas han pasado por aquí inútilmente.

Esta es sólo una regla, de las casi 1000 que tiene este router.

b) Puertos y protocolos inseguros en las reglas del FW.

Una medida de especial atención en un FW es el control de protocolos inseguros, uno de los reportes de esta herramienta presenta claramente empleo, por ejemplo de "telnet", como lo vemos a continuación:

22.	O07	TCP on over 2000 ports can exit your network	✗
23.	I04	Telnet can enter your network	✗

Si esto se compara con las reglas de ese FW, se puede encontrar:

```
access-list outside_access_in extended permit tcp object-group ONMOB
10.222.154.224 255.255.255.224 range ftp telnet

access-list outside_access_in extended permit tcp 10.255.243.0
255.255.255.0 10.222.154.224 255.255.255.224 range ssh telnet
```

Como se puede apreciar, no existe ningún comentario, descripción o referencia respecto a esta actividad. A su vez la dirección 10.222.154.224: Se trata de una dirección IP de otra red (que no es de la empresa que estamos revisando), en este ejemplo no se ha logrado identificar esta IP dentro del esquema de direccionamiento que administra el operador de esta red que estamos presentando según la información recibida.

Esta mera información debería despertar el interés de cualquier persona que realizara seguimiento con estos reportes. Si seguimos analizando los reportes en otro, también se puede apreciar lo siguiente:

	RULE	CHANGE TIME	CHANGED BY	SOURCE	DESTINATION	SERVICE	ACTION	SOURCE NAT	DESTINATION NAT
	acl(777)	3Aug2012 03:48:20	9808	ONMO	10.222.154.224/27	tcp:161-162	PASS	-	-
	acl(778)	3Aug2012 03:48:20	9808	ONMO	10.222.154.224/27	tcp:383	PASS	-	-
	acl(779)	3Aug2012 03:48:20	9808	ONMO	10.222.154.224/27	tcp:4459-4460	PASS	-	-
	acl(780)	3Aug2012 03:48:20	9808	ONMO	10.222.154.224/27	tcp:8080-8083	PASS	-	-
	acl(781)	3Aug2012 03:48:20	9808	ONMO	10.222.154.224/27	tcp:21-23	PASS	-	-
	acl(782)	3Aug2012 03:48:20	9808	ONMO	10.222.154.224/27	www	PASS	-	-
	acl(783)	3Aug2012 03:48:20	9808	ONMO	10.222.154.224/27	tcp:1433	PASS	-	-

El día 03 de agosto de 2012 un usuario "9808" cambió toda una secuencia de permisos "peligrosos" telnet, ftp, snmp, mysql, web, etc. Para hosts supuestamente de una IP que no conocemos y ¿no está quedando rastro de orden de trabajo, tickets, notificaciones, GUI asentado en ninguna parte de este FW?

Este tipo de trabajo demuestra que no se está explotando la herramienta como se podría llegar a hacer y esta ausencia de tareas impacta en forma directa con la eficiencia y/o disponibilidad de la red y la seguridad de los accesos. A su vez se pone de manifiesto que no se está cumpliendo con el hecho de dejar constancia de tareas o modificaciones en las políticas del FW, pues debería contar con alguna descripción o comentario que haga referencia a la existencia de algún tipo de ticket o flujo que haya autorizado esta acción

c) Empleo de reglas excesivamente "holgadas".

Otro de los informes de esta herramienta presenta una clara evidencia de empleo de reglas que deberían ser mucho más restrictivas. En este caso se trata del FW que debería estar protegiendo la interconexión con el resto de empresas con las que trabaja esta organización, el FW es "M-F535-01B". Como se puede ver en el informe existen reglas que permiten el paso a determinados grupos de objetos:

Trust outside_access_in(92)	1 1 2	access-list outside_access_in remark PRODUCCION access-list outside_access_in extended permit ip object-group SVC_A object-group P2	279,992
Trust outside_access_in(93)	1 1 2	access-list outside_access_in extended permit ip object-group VO_MA object-group P2T	656
Trust outside_access_in(94)	1 1 2	access-list outside_access_in remark DESARROLLO MOVITALK access-list outside_access_in extended permit ip object-group P2TS_D object-group P2T_D	577,023

Si se buscan estas reglas en la configuración del FW se aprecia lo siguiente:

access-list outside_access_in extended permit ip object-group SVC_A object-group P2

(Idem con: access-list outside_access_in extended permit ip object-group VO_MA object-group P2T)

<u>CONCLUSIÓN 1</u>: Se está permitiendo acceso directamente a nivel "IP", es decir que puede establecerse conexiones TCP y/o UDP hacia cualquiera de los **65.535** puertos.

Cuando buscamos de qué Object Groups se tratan, se encuentra lo siguiente:

```
object-group network SVC_A
 group-object P2TA
 group-object PT2B
 group-object PT2C
 group-object PT2D
 group-object PT2E
 group-object PT2F
 group-object PT2G
 group-object PT2H

object-group network P2
 network-object host 10.216.45.13
 network-object host 10.216.45.14
 network-object host 10.216.45.15
 network-object 10.216.45.16 255.255.255.240
 network-object 10.216.45.32 255.255.255.248
 network-object host 10.216.45.123
 network-object 10.216.45.128 255.255.255.224
 network-object 10.216.45.124 255.255.255.252
 network-object host 10.216.45.40
 network-object host 10.216.45.41
 network-object host 10.216.45.42

object-group network PT2C
 network-object host 10.183.0.103
 network-object host 10.183.0.104
 network-object host 10.183.0.105
 network-object host 10.183.0.106
 network-object host 10.183.0.107
 network-object host 10.183.0.108
 network-object host 10.183.0.109
 network-object host 10.183.0.110
 network-object host 10.183.0.111
 network-object host 10.183.0.112

object-group network PT2E
 network-object host 10.24.178.36
 network-object host 10.24.178.37
 network-object host 10.24.178.38
 network-object host 10.24.178.39
 network-object host 10.24.178.40
 network-object host 10.24.178.41
 network-object host 10.24.178.42
 network-object host 10.24.178.43
 network-object host 10.24.178.44
```

```
 network-object host 10.24.178.45
 network-object host 10.24.178.46

object-group network PT2F
 network-object host 10.116.251.145
 network-object host 10.116.251.146
 network-object host 10.116.251.147
 network-object host 10.116.251.148
 network-object host 10.116.251.149
 network-object host 10.116.251.150
 network-object host 10.116.251.151
 network-object host 10.116.251.152
 network-object host 10.116.251.153
 network-object host 10.116.251.154

object-group network PT2G
 network-object 10.29.60.192 255.255.255.240
 network-object host 10.29.60.207
 network-object host 10.29.60.208
 network-object host 10.29.60.209
 network-object host 10.29.60.210
 network-object host 10.29.60.211
 network-object host 10.29.60.212
 network-object host 10.29.60.213
 network-object host 10.29.60.214
 network-object host 10.29.60.215
 network-object host 10.29.60.216
 network-object host 10.29.60.217
 network-object host 10.29.60.218
 network-object host 10.29.60.219
 network-object host 10.29.60.220
 network-object host 10.29.60.221
 network-object host 10.29.60.222
 network-object host 10.29.60.223
```

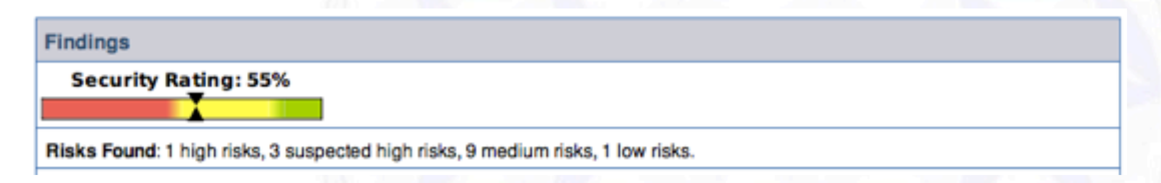
CONCLUSIÓN 2: Se está permitiendo el paso desde esas direcciones y rangos de red externas a la organización sin ninguna restricción, hacia varios rangos de direcciones de la propia empresa.

El reporte de Algosec, está informando con toda claridad que estas reglas poseen un riesgo alto ("**High**"), sin embargo no se adoptan medidas para "ajustar" las mismas. Es muy poco probable que exista la necesidad de abrir estos rangos de direcciones IP hacia la totalidad de los puertos.

Cuando esto se suma a varias direcciones IP más que también de forma más puntual permiten acceso a diferentes puertos (*tal cual figura también en estos reportes*), se están dejando abiertas varias puertas que sumadas aumentan las vulnerabilidades.

d) Planes de acción o planes de mejora sobre lo que presentan los reportes.

La adquisición de este tipo de herramientas implica un "proceso". De poco sirve poder evaluar el nivel de seguridad de una infraestructura, si ello queda paralizado en un reporte. La mayor potencialidad que ofrecen las mismas es la de "**Gestión de la Seguridad**" como un ciclo de vida, tal cual lo establecen los actuales estándares de seguridad. Como se puede ver a continuación, los reportes informan un umbral que es demasiado bajo (*casi al límite*) para ser aceptado, sin embargo en esta empresa, no se ha encontrado una metodología de seguimiento, hitos o acciones de mejora.



6.12. Empleo de máquinas de salto.

Una máquina de salto, no es más que un dispositivo con, al menos, dos interfaces físicas de red, sobre las cuáles configuramos *diferentes rangos de direccionamiento IP*, por ejemplo llamémosla ***red externa*** y ***red interna***. El **factor de éxito** es que en nuestro caso la "red interna" no posea absolutamente ninguna "puerta de entrada" que no sea a través de esta máquina de salto, este es el único concepto que no puede ser alterado.

Su objetivo fundamental es "**separar**" ambas redes de forma tal, que cualquier usuario que desee ingresar, en nuestro ejemplo hacia la "red interna", deba primero validarse en este host (máquina de salto) y luego, situado dentro de este host ya tendrá visibilidad hacia la red interna, pues en realidad estará ejecutando los comandos desde la máquina de salto misma.

Este tipo de conceptos aplica particularmente sobre lo que ya hemos denominado y presentado al principio del libro como "**redes de gestión**". Estas redes, como su nombre lo indica, son las que nos permitirán acceder a los diferentes elementos para realizar cualquier tipo de tarea de configuración, administración, supervisión y mantenimiento, y en una red debidamente segmentada, hacia estas redes sólo deberán acceder los usuarios autorizados para ello y nadie más. Son las redes "plenipotenciarias" de toda la organización.

Todo dispositivo de red, puede estar ofreciendo a través de sus interfaces los servicios que haga falta o para los que fue diseñado, pero debería tener una interfaz (*en lo posible física*) específicamente configurada para su acceso de gestión. Sólo sobre esa interfaz es que debemos abrir los puertos necesarios para gestionar el elemento, y en nuestro ejemplo, este podría ser el segmento IP correspondiente a la "red interna". No debería existir **ninguna posibildad** (*reiteramos: "**Ninguna posibilidad**")*, de ejecutar tareas de gestión sobre los dispositivos a través de otra interface.

La primer ventaja entonces, que nos ofrece una máquina de salto, es la de ser la "única puerta de entrada" hacia la red de gestión en este caso o la red destino que deseamos segmentar. La segunda ventaja es que sobre esa máquina de salto, únicamente el administrador (*o el área de administración de la misma*) es quien posee el acceso como "**root**", por lo tanto será la única persona que crea las cuentas de usuarios a los que se les permitirá acceder a la red destino. Una de sus principales responsabilidades es el ABM (Alta - Baja – Modificación) de usuarios, pudiendo enjaularlos dónde desee y como cuestión muy importante: configurando el sistema de "SysLog" de esta máquina de salto para que almacene toda la actividad de conexión y de comandos que cada usuario ejecute desde su cuenta, lo cual nos ofrece un tercer aspecto de seguridad que es la **trazabilidad** de todos los usuarios. Por supuesto que, como ya hemos comentado, es fundamental exportar estos Logs hacia un servidor de Logs externo o plataforma SIEM.

Hasta ahora estamos presentando esta solución para usuarios que deseen realizar accesos vía "Línea de Comandos", es decir por SSH (*por telnet ni siquiera lo mencionaremos….*), pero ¿qué sucedería si los usuarios necesitan ingresar a dispositivos finales que poseen interfaz gráfica? Para esta actividad aún nos queda la posibilidad de permitirles a esos usuarios realizar "Redirección de puertos" a través del protocolo SSH, este tema lo desarrollaremos en el capítulo final de "Trabajo con determinados Comandos y herramientas".

A continuación presentamos una imagen de ejemplo sobre cómo sería el emplazamiento y esquema de direccionamiento de una máquina de salto que segmente dos zonas de red o dos redes.

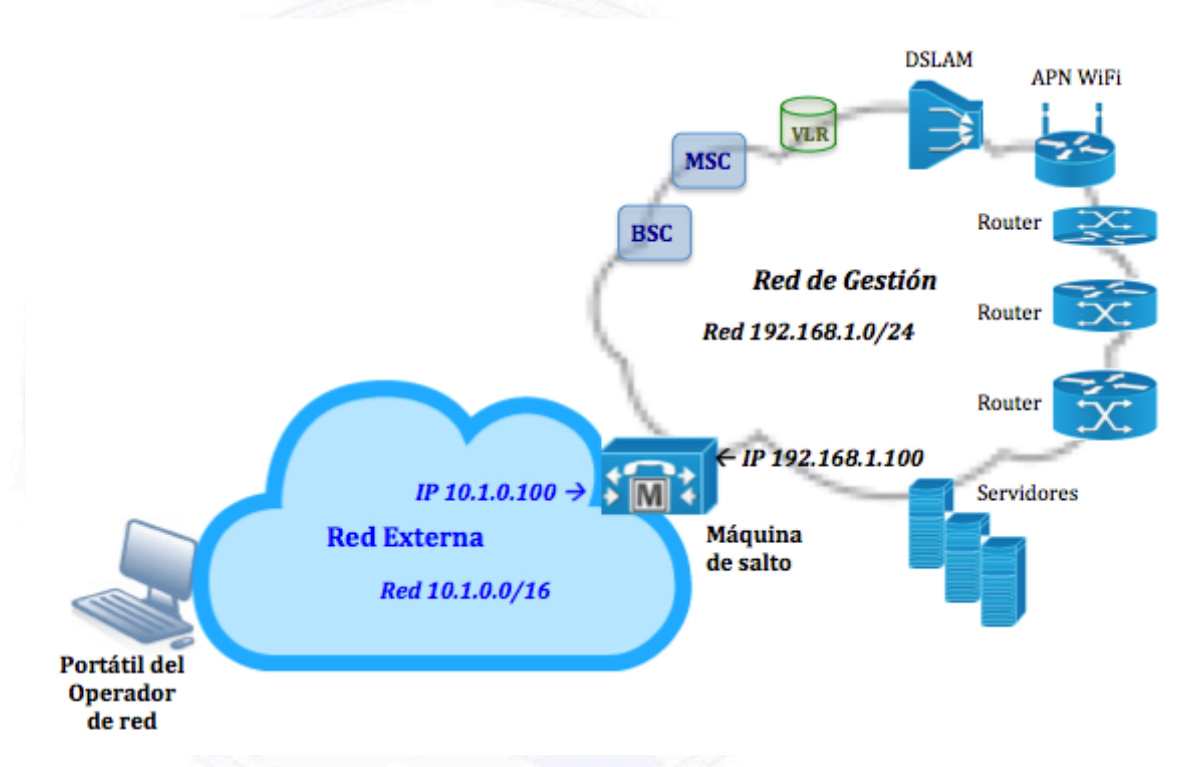


Imagen 6.43 (Ejemplo de despliegue de una máquina de salto)

7. Empleo de protocolos inseguros

7.1. Presentación

Este tema es muy frecuente en casi todas las redes, es una mala práctica habitual de la masa de los administradores de red que llevan años en el tema, seguramente intentarán presentarnos varias excusas y justificaciones para su empleo y para nosotros será de suma importancia pues es uno de los mayores focos de conflicto.

En este capítulo, si bien existe una larga lista de protocolos que son explotables y nos debilitan nuestra seguridad, intentaremos presentar los que con mayor frecuencia solemos encontrar como casi "omnipresentes" en la mayoría de las redes.

7.2. Telnet

En este protocolo, toda la información viaja en texto plano, tanto los comandos que el operador ejecuta como las respuestas de ese host, por lo tanto con cualquier herramienta de escucha es posible capturar la información necesaria para conectarse con los mismos privilegios que ese operador.

El protocolo de gestión seguro que debería emplearse es "**SSH**" (Secure SHell), el mismo permite mecanismos de autenticación robusta y criptografía desde el mismo control de acceso hasta el cierre de sesión. Existen aún algunos dispositivos antiguos que no admiten "ssh", exclusivamente en esos casos debería estar perfectamente identificados y justificado por escrito el empleo de telnet.

A continuación presentamos una imagen que, aprovechando el "análisis de flujo" de la herramienta "Wireshark", pone al descubierto el acceso de un usuario con s respectiva password:

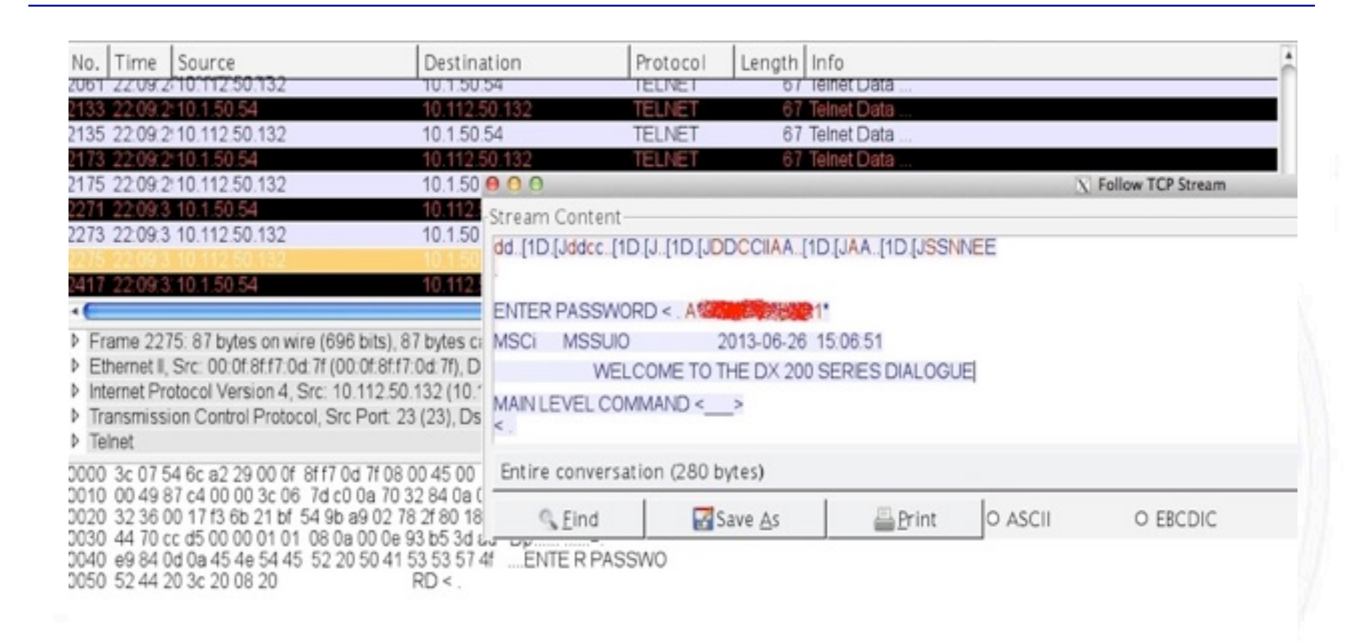


Imagen 7.1 (Ejemplo de captura protocolo telnet)

En la imagen anterior, hemos realizado una captura con “Wireshark” luego filtrado por protocolo “telnet”, y finalmente con la opción de “*Follow TCP stream*” reconstruimos toda la sesión, y como se puede ver en la imagen (*aunque lo hemos tachado en rojo*) en esa ventana aparece la password de ese usuario en texto plano.

7.3. ftp (file Transfer Protocol)

Al igual que en el caso anterior (*telnet*), para la transferencia de archivos, se suelen emplear protocolos inseguros, también aquí los comandos del operador, su nombre de usuario y contraseña, como también los archivos que se transportan lo hacen sin ningún tipo de seguridad, es decir en texto plano.

Veamos algunas capturas de tráfico de este protocolo.

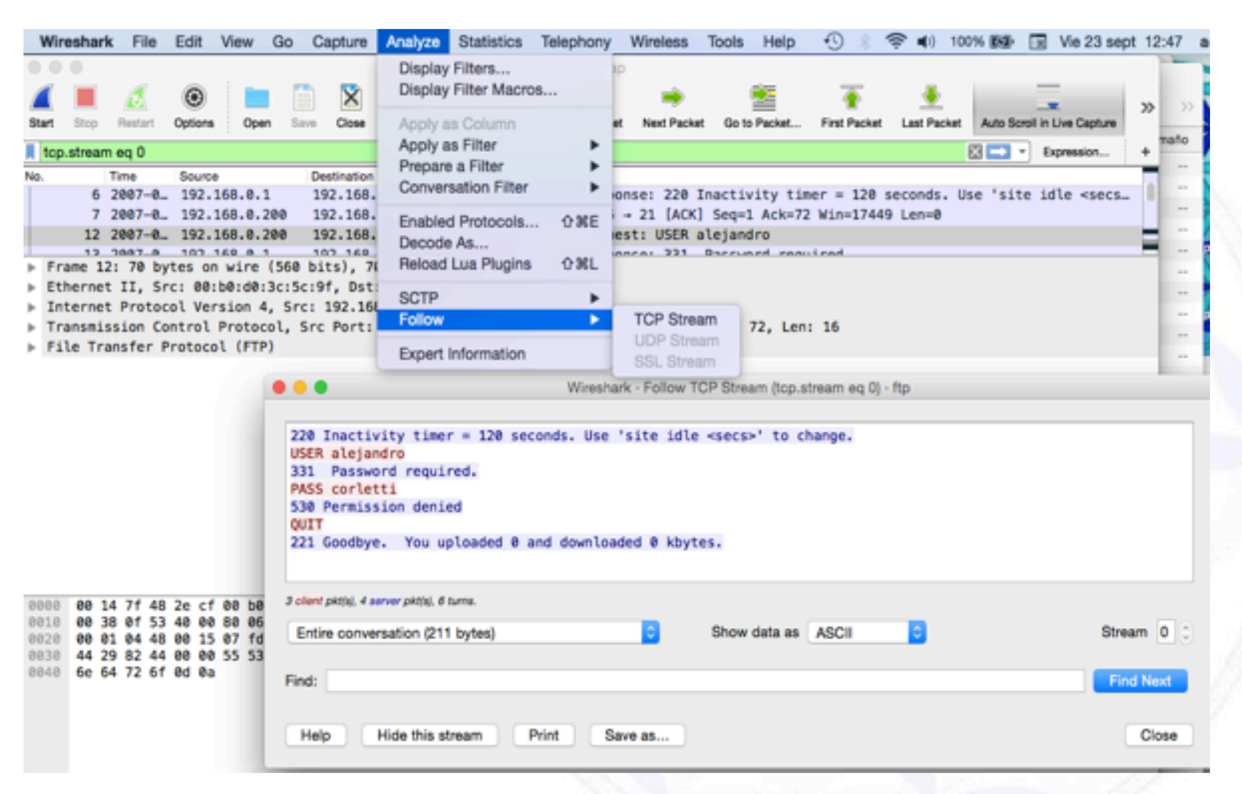


Imagen 7.2 (Ejemplo de captura protocolo ftp)

En la imagen anterior, podemos apreciar una captura en la cual se filtró un flujo específico "ftp" (*tcp.stream eq 0*) y se seleccionó realizar un seguimiento del mismo (*Follow TCP Stream*). Abajo y al derecha vemos la ventana emergente de esta flujo, y dentro de la misma en texto plano "*USER alejandro*" y más abajo "*PASS corletti".* Este flujo si bien responde "*Permission denied*", nos demuestra cómo al capturar tráfico en nuestra red, este protocolo no emplea ninguna medida de seguridad, transmitiendo toda la información en texto plano.

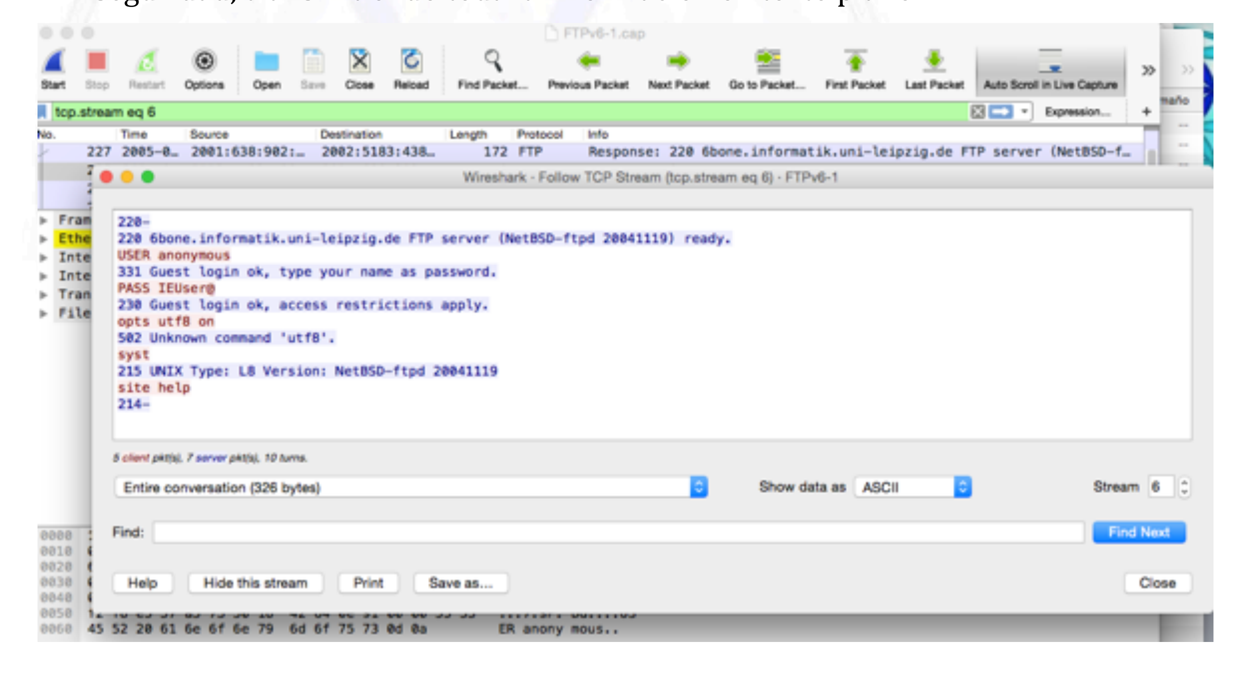


Imagen 7.3 (Ejemplo de captura protocolo ftp)

Quisimos presentar también la imagen anterior, pues si prestamos atención se trata de protocolo "ftp" pero trabajando sobre **IP versión 6**, y como podemos corroborar en la misma, también ftp sobre IPv6 trabaja en texto plano. Un detalle que podemos apreciar también, es que en la parte inferior de la imagen (*que se corresponde con la presentación en hexadecimal que nos ofrece Wireshark dentro de sus tres ventanas de captura*) se lee con total claridad la palabra "anonymous", lo que estamos viendo aquí es que en la trama 228 que es la que aparece en la ventana posterior de Wireshark, viaja concretamente el nombre del USER, y su correspondencia en texto plano de los byte (que figuran abajo a la izquierda) en hexadecimal: 61=a, 6e=n, 6f=o, 6e=n, 79=y, 6d=m, 6f=o, 75=u, 73=s.

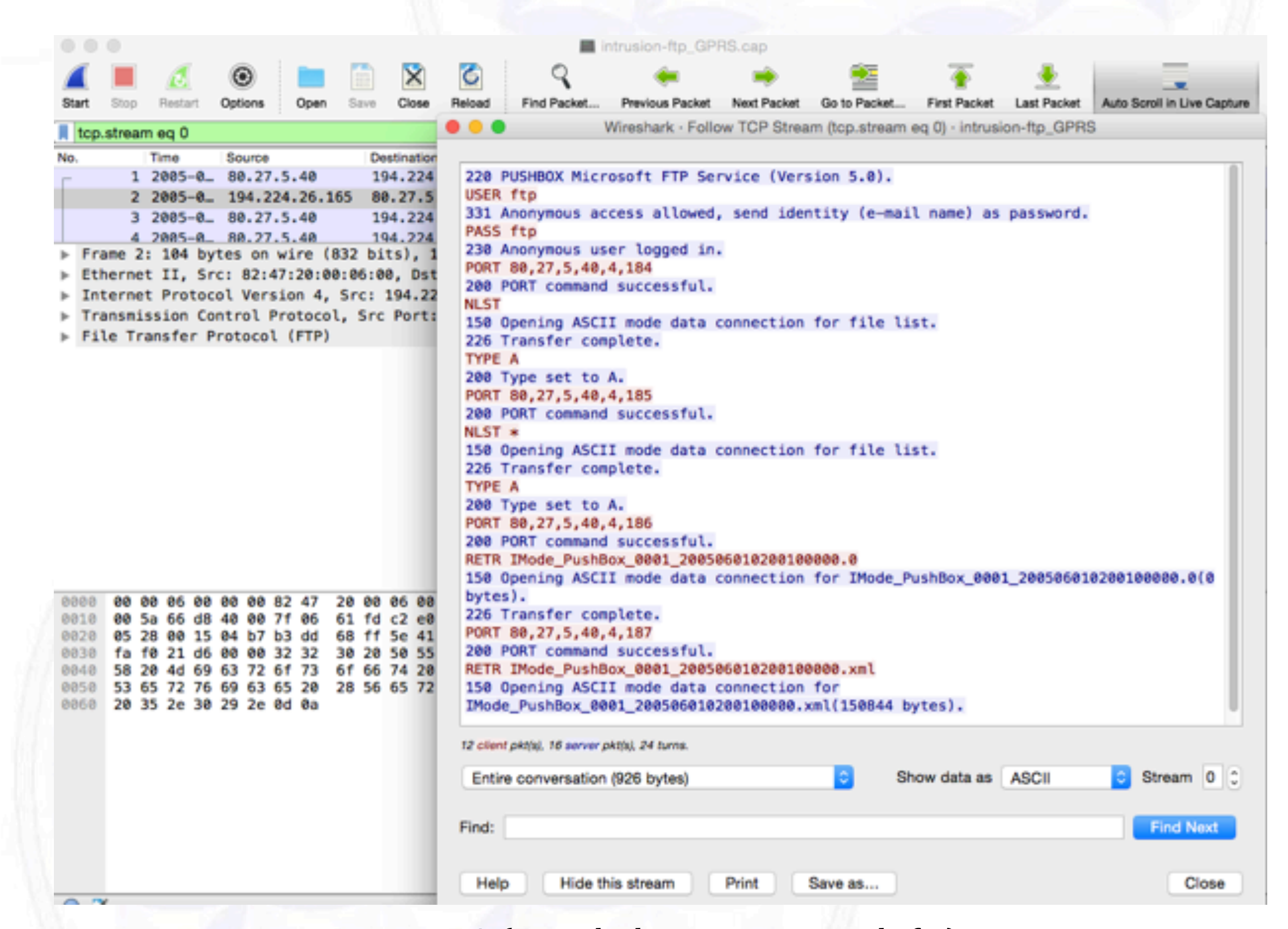


Imagen 7.4 (Ejemplo de captura protocolo ftp)

Por último queremos presentar la imagen anterior y la siguiente, para que no pasemos por alto que el protocolo ftp emplea dos puertos: el TCP 21 para comandos y el TCP 20 para transferencia de información. Cuando se desea hacer un seguimiento serio de la actividad de ftp (*que en muchos casos es fundamental para análisis forense*), se debe hacer el seguimiento, o dejar escuchando tráfico sobre ambas "sesiones" pues

cada una de ellas establece un triple handshake por separado: una sesión hacia el puerto **21**, y luego otra hacia el puerto **20**, como podemos apreciar en estas dos imágenes.

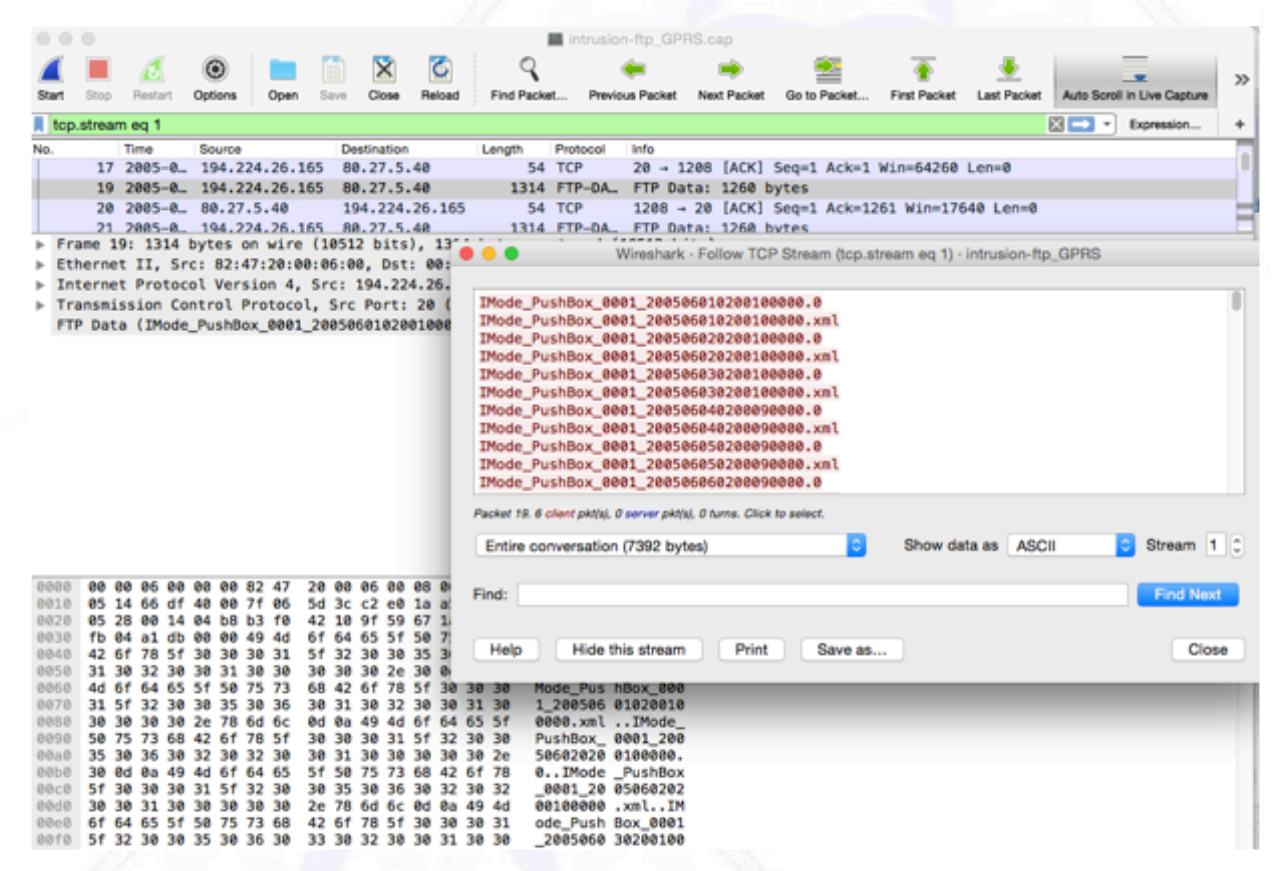


Imagen 7.5 (Ejemplo de captura protocolo ftp)

7.4. SNMP versión 1 (Single Network Monitor Protocol)

El protocolo SNMP versión 1 como cabe esperar, es la versión inicial del mismo, a finales de los años 90` ya se conocían un gran número de vulnerabilidades que permitían obtener información indebidamente de alto detalle sobre cualquier dispositivo por medio del empleo del mismo. La versión dos mejoró todos ellos, pero aún ofrecía la debilidad de que no existía una autenticación robusta y que los datos viajaban en texto plano. Recién la versión tres aplicó conceptos de criptografía robusta (simétrica y asimétrica) tanto para el acceso (o autenticación entre cliente y servidor) como para la transmisión de la información, por esta razón debe ser actualizado sin falta al menos a la versión 2 (de ser posible a la 3), y por supuesto modificar la comunidad por defecto ("public"), nuevamente podemos recurrir al libro "**Seguridad por Niveles**" para una descripción detallada de los cambios que ofrece la versión 3.

Este protocolo de suma importancia para la monitorización y supervisión de red, por ofrecer mucha información a cualquiera que pueda "escucharlo" es que actualmente no se debe emplear en versiones anteriores a la 3, y de hecho la gran mayoría de los dispositivos actuales la soporta.

De encontrarse presente esta versión, en la configuración de los routers debería estar claramente de manifiesto (*Ejemplos para Cisco: #snmp-server user **** v3 auth md5 "secret" access 20, #snmp-server group ****** v3 noauth read sysonly, #snmp-server user ******* v3*), (*Ejemplos para Juniper: snmp v3, snmp v3 snmp-community community-index, snmpv3 access group*)

En la imagen siguiente, podemos apreciar cómo en una captura de tráfico se aprecia el empleo de la versión 1, y en la última línea se ve en texto plano el nombre de la comunidad que emplea.

62198	15:13:50	10.5.5.7	192.168.10.54	SNMP	270 Source port: 161
89755	15:13:52	10.5.5.7	192.168.10.54	SNMP	270 Source port: 161
110132	15:13:53	10.5.5.7	192.168.10.54	SNMP	269 Source port: 161
120522	15:13:53	10.5.5.1	192.168.10.54	SNMP	273 Source port: 161
122950	15:13:54	10.5.5.1	192.168.10.66	SNMP	136 get-response
132793	15:13:54	10.5.5.1	192.168.10.54	SNMP	272 Source port: 161
143076	15:13:55	10.5.5.1	192.168.10.54	SNMP	270 Source port: 161
155677	15:13:55	10.5.5.1	192.168.10.54	SNMP	268 Source port: 161

Frame 62198: 270 bytes on wire (2160 bits), 100 bytes captured (800 bits)
Ethernet II, Src: 00:1c:b0:5b:55:40 (00:1c:b0:5b:55:40), Dst: 01:00:5e:10:6a:03 (01:00:5e:10:6a:03)
Internet Protocol Version 4, Src: 10.18.192.130 (10.18.192.130), Dst: 10.53.231.54 (10.53.231.54)
User Datagram Protocol, Src Port: 1701 (1701), Dst Port: 1701 (1701)
Layer 2 Tunneling Protocol
Point-to-Point Protocol
Internet Protocol Version 4, Src: 10.5.5.7 (10.5.5.7), Dst: 192.168.10.54 (192.168.10.54)
User Datagram Protocol, Src Port: 161 (161), Dst Port: 161 (161)
Simple Network Management Protocol
version: version-1 (0)
community: h0ng

Imagen 7.6 (Ejemplo de captura protocolo snmp v1)

Una buena opción también para evaluar el empleo de este protocolo o al menos qué dispositivos lo emplean, es a través del comando "**nmap**":

snmp usando nmap:

```
sh-3.2# nmap -sU -p 161 IP/Red_destino -sV
```

O también con el comando "snmpwlak"

```
sh-3.2# snmpwalk -c public -v 1 IP_destino system
```

7.5. NetBIOS

El protocolo NetBIOS, es un protocolo propietario de Microsoft que se emplea para la resolución de nombres de esta empresa y el tráfico ente cliente y servidor. No tiene sentido su empleo fuera de un entorno LAN.

Este tipo de protocolos es el que viene configurado por defecto al instalar cualquier Sistema Operativo de la familia Windows, cuando no se hace un riguroso bastionado de las máquinas, existe una importante cantidad de información de usuarios y configuraciones viajando en texto plano por la red. En el caso de una red de pequeña empresa, tal vez no sea tan importante, pero sí lo es en un los segmentos de "Gestión/Administración" de los elementos de core o críticos de una gran red.

Cuando existe alta frecuencia del empleo de estas familias de protocolos indica con claridad la falta de bastionado de equipamiento cliente (y también posiblemente servidores), por lo tanto si no se incrementan las medidas de seguridad de los mismos, al comprometer cualquiera de ellos, se posee una puerta directa hacia los elementos finales a administrar.

En entornos de producción y redes más complejas, no tiene mucho sentido el empleo del mismo, a lo sumo puede ser usado por determinados servidores que estén correctamente configurados (*y ajustados en su seguridad*).

El empleo indiscriminado de estos protocolos, ofrece información importante para quien quiera recolectarla y es el primer paso para un intruso denominado "Finger printing" y a su vez abre las puertas para el segundo paso "Foot printing", donde ya obtenemos: Usuarios, contraseñas, recursos, jerarquías, redes, servidores, etc..

Como se presentará a continuación, en varias de las redes que hemos conocido, se detecta un alto consumo del tráfico de red con este protocolo el cual ofrece la información que se presenta a continuación.

Primero podemos ver aquí abajo la imagen de esta captura donde se aprecia la ocurrencia de este protocolo "NBNS", en esta imagen el puerto **TCP 137**, y a la derecha de la misma se pueden apreciar en texto plano los nombres de usuarios/hosts seguidos por el décimo sexto carácter <00>, <20> temas que desarrollamos a continuación. En la captura que sigue hemos eliminado bastantes caracteres del Nombre NetBIOS pero puede apreciarse con claridad el décimo sexto carácter <00> o <20>.

En pocos segundos de captura se han generado cientos de tramas con este protocolo, de las cuales como se verá capturamos cientos de nombres también.

No.	Time	Source	Destination	Protocol	Length	Info
5066	20:02:4	10.112.196.17	10.112.196.127	NBNS	92	Name query NB IS P<00>
5064	20:02:4	10.112.196.17	10.112.196.127	NBNS	110	Registration NB U I7LEARIAS<00>
5063	20:02:4	10.112.196.17	10.112.196.127	NBNS	110	Registration NB O EL<00>
5062	20:02:4	10.112.196.17	10.112.196.127	NBNS	110	Registration NB U I7LEARIAS<20>
5060	20:02:4	10.112.196.12	10.112.196.127	NBNS	92	Name query NB O ELALTIRIS<00>
5059	20:02:4	10.112.196.17	10.112.196.127	NBNS	92	Name query NB O ELALTIRIS<00>
5058	20:02:4	10.112.196.17	10.112.196.127	NBNS	92	Name query NB IS P<00>
5050	20:02:4	10.112.196.17	10.112.196.127	NBNS	110	Registration NB O EL<00>
5049	20:02:4	10.112.196.17	10.112.196.127	NBNS	110	Registration NB U I7LEARIAS<00>
5048	20:02:4	10.112.196.17	10.112.196.127	NBNS	110	Registration NB U I7LEARIAS<20>
5036	20:02:4	10.112.196.12	10.112.196.127	NBNS	92	Name query NB O ELALTIRIS<00>
5025	20:02:4	10.112.196.12	10.112.196.127	NBNS	92	Name query NB O ELQ03<20>
5012	20:02:4	10.112.196.12	10.112.196.127	NBNS	92	Name query NB O ELALTIRIS<00>
5004	20:02:4	10.112.196.12	10.112.196.127	NBNS	92	Name query NB O... ELQ03<20>

- Frame 5048: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
- Ethernet II, Src: b4:99:ba:e0:b5:b5 (b4:99:ba:e0:b5:b5), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 10.112.196.17 (10.112.196.17), Dst: 10.112.196.127 (10.112.196.127)
- User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
- NetBIOS Name Service

Imagen 7.7 (Ejemplo de captura protocolo NetBios)

Décimo sexto carácter NetBIOS:

Este carácter, que es el último de los dos octetos de los "Nombres NetBIOS" nos dice qué servicio está ofreciendo ese host, cuestión clave para determinar el rol de cada uno de ellos. A continuación se presenta un breve resumen de lo detectado:

<1B> Examinador principal de Dominio.

A continuación, presentamos un ejemplo de secuencias de tramas capturadas las que desplegamos al completo, en las mismas se aprecia el rol y nombre del Examinador principal de Dominio.

```
    17:43:12.804703 10.112.203.51           10.112.203.127          NBNS      92
Name query NB INIMS<1b>

    Ethernet    II,    Src:    6c:3b:e5:12:ee:5f    (6c:3b:e5:12:ee:5f),    Dst:
ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Internet  Protocol  Version  4,  Src:  10.112.203.51  (10.112.203.51),  Dst:
10.112.203.127 (10.112.203.127)
    User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
    NetBIOS Name Service
        Transaction ID: 0x9418
        Flags: 0x0110 (Name query)
        Questions: 1
        Answer RRs: 0
        Authority RRs: 0
        Additional RRs: 0
        Queries
            INICIOMS<1b>: type NB, class IN
                 Name: INIMS<1b> (Domain Master Browser)
                Type: NB
```




```
                Class: IN

     142 17:43:24.065564 10.112.203.51         10.112.203.127        NBNS      92
Name query NB XXXXXX <1b>

     Ethernet    II,    Src:    6c:3b:e5:12:ee:5f    (6c:3b:e5:12:ee:5f),    Dst:
ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
     Internet  Protocol  Version  4,  Src:  10.112.203.51  (10.112.203.51),  Dst:
10.112.203.127 (10.112.203.127)
     User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
     NetBIOS Name Service
         Transaction ID: 0x9423
         Flags: 0x0110 (Name query)
         Questions: 1
         Answer RRs: 0
         Authority RRs: 0
         Additional RRs: 0
         Queries
             XXXXXX<1b>: type NB, class IN
                 Name: XXXXXX<1b> (Domain Master Browser)
                 Type: NB
                 Class: IN


         173 17:43:26.630415 10.112.203.51          10.112.203.127          NBNS
92     Name query NB GRUPOOSS<1b>

     Frame 173: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
     Ethernet    II,    Src:    6c:3b:e5:12:ee:5f    (6c:3b:e5:12:ee:5f),    Dst:
ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
     Internet  Protocol  Version  4,  Src:  10.112.203.51  (10.112.203.51),  Dst:
10.112.203.127 (10.112.203.127)
     User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
     NetBIOS Name Service
         Transaction ID: 0x9426
         Flags: 0x0110 (Name query)
         Questions: 1
         Answer RRs: 0
         Authority RRs: 0
         Additional RRs: 0
         Queries
             GRUPOGSS<1b>: type NB, class IN
                 Name: GRUPOOSS<1b> (Domain Master Browser)
                 Type: NB
                 Class: IN
```

A continuación presentamos otros ejemplos en los cuáles hemos seleccionado el décimo sexto caracter <20>: Servidor de archivos (*que nos indica que posee archivos compartidos*)

```
       232 17:43:29.889867 10.112.203.34         10.112.203.127        NBNS      92
Name query NB YYP0SA<20>
     Ethernet    II,    Src:    88:ae:1d:b4:0d:7c    (88:ae:1d:b4:0d:7c),    Dst:
ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
```

```
     Internet Protocol Version 4, Src: 10.112.203.34 (10.112.203.34), Dst: 10.112.203.127 (10.112.203.127)
     User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
     NetBIOS Name Service
         Transaction ID: 0xb2bb
         Flags: 0x0110 (Name query)
         Questions: 1
         Answer RRs: 0
         Authority RRs: 0
         Additional RRs: 0
         Queries
             4RD1P06DVSS<20>: type NB, class IN
                 Name: YYP0SA<20> (Server service)
                 Type: NB
                 Class: IN

        286 17:44:27.617562 10.112.203.23          10.112.203.127          NBNS
92      Name query NB YYP09NA01<20>

     Frame 286: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
     Ethernet II, Src: e4:11:5b:4b:57:d8 (e4:11:5b:4b:57:d8), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
     Internet Protocol Version 4, Src: 10.112.203.23 (10.112.203.23), Dst: 10.112.203.127 (10.112.203.127)
     User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
     NetBIOS Name Service
         Transaction ID: 0xd610
         Flags: 0x0110 (Name query)
             0... .... .... .... = Response: Message is a query
             .000 0... .... .... = Opcode: Name query (0)
             .... ..0. .... .... = Truncated: Message is not truncated
             .... ...1 .... .... = Recursion desired: Do query recursively
             .... .... ...1 .... = Broadcast: Broadcast packet
         Questions: 1
         Answer RRs: 0
         Authority RRs: 0
         Additional RRs: 0
         Queries
             4RD1P09AQ10024<20>: type NB, class IN
                 Name: YYP09NA01<20> (Server service)
                 Type: NB
                 Class: IN
```

A continuación presentamos un ejemplo más en el cuál hemos seleccionado el décimo sexto caracter <1C> Controlador de dominio

```
       968 18:24:21.721598000 10.1.31.48            10.1.31.255            NBNS
92      Name query NB XXXXXX<1c>

     Ethernet II, Src: 00:21:9b:39:a8:fc (00:21:9b:39:a8:fc), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
     Internet Protocol Version 4, Src: 10.1.31.48 (10.1.31.48), Dst: 10.1.31.255 (10.1.31.255)
```

```
User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
NetBIOS Name Service
……
…
.
```

<u>Nombres de hosts/usuario</u>.

Durante un brevísimo período de captura en una red se han detectado cientos de nombres de usuario (*Suele ser una constante en este protocolo, que <u>estos mismos nombres se empleen para el acceso a varios servicios de la red</u>, por lo tanto el próximo paso de un intruso, es pasarlos a un "**diccionario**" y con el empleo del mismo tiene altas probabilidades de acceder a los servicios/recursos de la red*).

Por supuesto <u>hemos modificado de todos ellos los que identifican fehacientemente usuario</u>, sólo se presentan a título de ejemplo como representativo del "volumen" de información que nos ofrece este protocolo en pocos minutos

```
      ADITA  ADITATEST  ATIIIA  VENUSBD  VENUSDC01  VENUSECUVM01  VENUSECUVM02   VENUSECUVM03  VENUSECUVAD7
VENUSECUVP0N  VENUSECUVRT9  VENUSECUVJJU  VENUSECUVIOP   VENUSECUV123  VENUSECUVas0  VENUSECUVas1  VENUSECUVas2
VENUSECUVas3  VENUSECUVas4   VENUSECUVas5  VENUSECUVas6  VENUSECUVas7  VENUSECUVas8  VENUSECUVas9  VENUSECUVM20
VENUSECUVM21  VENUSECUVM22  VENUSECUVM23  VENUSWI01   VENUSWI02MM  B  QBLD02     BQBLD04   BQDOC2  CALLPILOT
CONWWHTM66  CONSDMIUXI   SasV000VWGH  SasVas007X  Sas0040P8W  SasVasAD  SasVasPFC    SESSVas00QAPRU  SasVDD001
Sas00Sas04  SasV00S3561  SasVas00asTYS  SasVas0045Z  SasVas002134S  SasVas00WasQ  V  SasVas00SNDQA  CONSSFV7
CONS725VR   CONSPRUEB   NSULL4RD1SasS4   CO45Q1002693   CO45PBLJUESCAND   CORasYNA002125   CORADFHA002263
CORAPBLNA002781     CORAPBLNA002849   CORAPBLNA176844   CORAPBL8QWas4426   CORAPBLNWasT0199   CORCasTAVS8143
CORC01DKIOSKO05    CORCPBDCAVS04    CORCPBDCAVS06    CORCPBDCADF10    CORCPBDASDFVS1N02    CORCPBDCAVS31XY
CORCPBDCAVS4CG1   CORCPBDCAVS733Z   CORCPBDCAVS7DHZ    CORCPBDQWECSJFP5   CORCPBDCAVSKTG1   CORCPBDCAVSRSAC
CORCPBDCAVSZTG1     CORCPBDELHOYOS   CORCPBAQ1001290   CORCPBAQ1002126   CORCPBAQ1002357   CORCPBAQ1002822
CORCPBDOSRV03V5   CORCPBLNA002042   CORCPBSCAVS03   CORM01DDIMURRAY    CORMPBDCAVS1HBH     CORMPBAQ1002042
ROMM03ECKTLC   ROMMAMBCKE21  ROMMAMBCKT97   ROMMAMBCKTLC   ROMMCORHT  ROMMESMDUR01  ROMMESMDURG1  ROMMESMDURG7
ROMMESMDURas     ROMas234CKTL1   ROMMLAGMCS02   ROMMLAGMCS04   ROMMNAE50359   ROMMNAE58351     ROMMPORSUN48
ROMMPUYMCS25    ROMMPUYMIC25   ROMMPUYMIO02     ROMMPUYMIOCM    ROMMUIARGPC1   ROMMUIARGPC2   ROMM4RD1CBY01
ROMM4RD1CYBas   ROMM4RD1HTas5    ROMM4RD1HTM20   ROMM4RD1HTM22   ROMM4RD1MIO27   ROMM4RD1MIO75   ROMM4RD1RQLLO
ROMM4RD1SasBS  ROMM4RD1SVP99  ROMM4RD1SVPBB  ROMM4RD1URB65  ECTGUI1  ECTSRV1     ELVEAD132      ELVPEPAD143
IPS20PW  WIPBDCAVS20QK  IPBDCAVS20R7    1234IPBDCAVS2N02    1234IPBDCAVSQ3   1234IPBDKIOSKO  1234M01DEVEDR
1234M01DGEAGA  1234M01DMAQUE  1234M01AQ1002241  1234M01AQ1002424  1234M01DROBRAVO  1234M01LJAMOR  1234M01LINA
1234M0NA002095  1234M0NA002123  12JHLBOLIM  1234M02OMAY  1234MMRRA  1234JHLMPSCHE  1234JHLN0032  1234JHLNA777
1234JHLN0064     1234JHLNA002069    1234JHLNA0093    1234JHLNA0313    1234JHLNA002381    1234JHLNA002474
1234JHLNA002550     1234JHLNA0587     1234JHLNA002617     1234JHLNA002627   1234JHLNA002659   1234JHLNA00699
1234JHLNA002738  1234JHLNA002777  1234JHLNA00292  1234JHLNA097  1234JHLNA17593    1234JHLREALG   1234JHLVORVA
1234M02LCAALO  1234M02LJEZO        1234M02LNA002454        1234M02LNSHE     1234M02LSRANDA    1234M02LYECON
1234M03DKAND  1234M03ARA      1234M03AQ1002687  1234M03LACIA      1234M03LasCO      1234M03LALLO  1234M03LORA
1234M03LNA00202     1234M03LNA0048    1234M03LNA008     1234M03LNA002805  1234M03LNA002     1234M03LNA002947
1234M03LRFLO   1234M03LXPEDA  1234AD7RGas     1234AD7LNA778     1234RT9DDDO  1234RT9AQ1002722  1234RT9AQ1044
1234RT9DPCAL   1234RT9DVVOZ      1234M0RRONTTE   1234RT9LDRANO    1234RT9NTINO      1236LJGUIRR  124RT9LMNRRE
1234RT92013  1234RT9LNA002091  1234RT9LN407    1234RT9LN2628   1234RT9LNA002673  1234RT9LN02979   1234RT9L983
1234RT9LNA400008    1234RT9LN0320    1234RT9LOSO      1234MPBDSEY    1234MBDSEZ    1234MPB1820  1234SPBDCAVS02
1234SPBDCA3     1234SPBDCA  04     1234SPBDCS07     1234SPBDCA8      1234SPBS09  1234SPBDC10      1234SPBDS11
1234SPBVS21  1234SPBREVAL  1234SPBAQ1002051  1234SP03V7         IVTA04002161      A04JOHSSSVAR  MTA04LMEEEYES
DDAQ104L2162  SSS4LWWW506  MNSSSS2314  MSSLN187  MNTMMOV08YC  XXXXXXA01     XXXXXXAFRODITA  XXXXXXAFRODITA2
XXXXXXAPLI03   XXXXXXAPLI04   XXXXXXAPPEFLOW1   XXXXXXAPPEFLOW2   XXXXXXAPPSP   XXXXXXAPPSVC01   XXXXXXAPPWas
XXXXXXAUDIT  XXXXXXB01    XXXXXXBACKUP01  XXXXXXBCM  XXXXXXBDD    XXXXXXBDDSP  XXXXXXBDDSVC01  XXXXXXBISOBJ01
XXXXXXBLCARRETA   XXXXXXBLCISCO   XXXXXXBLD13   o  XXXXXXBLD14   '  N  XXXXXXBLDM02   M  XXXXXXBLFREEWAY   L
XXXXXXBLMasAPP   '  2  XXXXXXBLMasDB       XXXXXXBOAPP  XXXXXXBOWEB  XXXXXXBUXIS01  XXXXXXCA1BO  XXXXXXCA1MNG
XXXXXXCADISTSRV    XXXXXXCQN    XXXXXXCSG01  XXXXXXCSG02  XXXXXXCTI01  XXXXXXCTI02  XXXXXXCTI03  XXXXXXCTI04
XXXXXXCTI05  XXXXXXCTIHA01  XXXXXXCTIHA02  XXXXXXCOCA  XXXXXXCVXP01  XXXXXXDATAFLOW  XXXXXXDFA01  XXXXXXDOMINO
XXXXXXEVEVA  XXXXXXEPINES  XXXXXXESX21  XXXXXXESXADM51  XXXXXXESXADMIN  XXXXXXELK    XXXXXXELK01  XXXXXXELK02
XXXXXXALK04   XXXXXXEQ01  XXXXXXEXC02  XXXXXXEX03  XXXXXXEX04  XXXXXXXCQ06   XXXXXXEQ07  XXXXXXEX08   XXXXXXFDE
XXXXXXFTPC  XXXXXXFEC02  XXXXXXGENTVIEW  XXXXXXGI   XXXXXXHTTP0123  XXXXXXIDM  XXXXXXICOM  XXXXXXTIL  XXXXXXLYN1
XXXXXXLYC02 XXXXXXYNC03 XXXXXXMCEE02 XXXXXXMRDP XXXXXXNIP XXXXXXNPPDC XXXXXXMONSas XXXXXXMONSSI XXXXXXDB01
XXXXXXRMS01  XXXXXXMSSCCM02  XXXXXXNES  XXXXXXNES02  XXXXXXNODDB01  XXXXXXCCVON  XXXXXXCOS03  XXXXXXPOS04
XXXXXXPPM  XXXXXXPPMAPP  XXXXXXPPMYQC  XXXXXXFFRINT  XXXXXXPROY01  XXXXXXQ01  XXXXXXQ02  XXXXXXQ03  XXXXXXQ04
```

XXXXXXQ05 XXXXXXRRRIADM XXXXXXRRRIDSHA XXXXXXRRRIFRW XXXXXXRRRIFRSA XXXXXXRRRIOUT XXXXXXRRRIOFVHA
XXXXXXRRRIREP XXXXXXRRRIREFFA XXXXXXRRRIURS XXXXXXRRRIURSA XXXXXXPIPSS1 XXXXXXPARPIPVV2 XXXXXXPARPIPCM3
XXXXXXPARPIPCS1 XXXXXXPARPIPCS2 XXXXXXPARPIPCS3 XXXXXXPARPIPCS4 XXXXXXPARPIPCS5 XXXXXXPARPMON
XXXXXXPARPVBN1 XXXXXXPARPWas1 C XXXXXXPARPWas10 XXXXXXPARPWas11 XXXXXXPARPWVV2 XXXXXXPARPWas14
XXXXXXPARPWas15 XXXXXXPARPWas16 XXXXXXPARPWBB7 XXXXXXPARPWas18 XXXXXXPARPWas19 XXXXXXPARPWas2
XXXXXXPARPWJK5 XXXXXXPARPWas6 XXXXXXPARPWas7 XXXXXXPARPWas8 XXXXXXQSIGGC XXXXXXQSIPCCHA XXXXXXQSIPGVP
XXXXXXQSIPGVPHA XXXXXXQSIPPRMHA XXXXXXQSIPRM XXXXXXSDT01 XXXXXXSEG01 XXXXXXSEG02 XXXXXXSEGFGGA
XXXXXXSETFPS XXXXXXSEGTGNNIM XXXXXXSEGGVBC01 XXXXXXGVP01 XXXXXXSHFSS2 XXXXXXSHP03 XXXXXXSHPOINT
XXXXXXSHPTEST XXXXXXSISCOM XXXXXXSPSVC01 XXXXXXSUPTEL01 XXXXXXTARIF XXXXXXETCOM XXXXXXTESTDXOW
XXXXXXTESCLOW XXXXXXTESTENE XXXXXXTETPPM XXXXXXTESTQA XXXXXXTESTRDDED XXXXXXTTSGC XXXXXXTESGC02
XXXXXXTESTSQL XXXXXXTMG01 XXXXXXTSTBXIS1 XXXXXXVENUS XXXXXXVMWADMIN XXXXXXWEB02 XXXXXXEBRasT
XXXXXXWEBSENSE XXXXXXWS01 XXXXXXWS02 XXXXXXWSUS XXXXXXXEN01 REGIOSRV SCLPREECVM01 SCLPROYEECUVM01 TEMX4RD1
4RD1A01CAVS5 4RD1A01DFFGG04 4RD1A01DCAVS06 4RD1AVS11 4RD1A0SSCCS12 4RD1A01DFFVS13 4RD1A01DCAVS8
4RD1A01DCAVS9 4RD1A01DCAVSRECE 4RD1A01DCST 4RD1AMEXC69 4RD1AMEPXXZG12 4RD1LY12DTAAES 4RD1M01FF17
4RD1M0AWAV25 4RD1M01DCAV26 4RD1M01DCAVMOD14 4RD1M01DAVS28 4RD1MCDXEPROANO 4RD1M01DOSNDSasV
4RD1M01LMALEON01 4RD1MXXA187393 4RD1JHLNA002295 4RD1M03DALPADIL 4RD1M03DELREVELO 4RD1MSADMGUAMAN
4RD1M03DMRIOSCG1 4RD1M03DMSAMANIE 4RD1MSCRAQ1002005 4RD1M03AQ1002081 4RD1M03AQ1002083 4RD1E34NA002087
4RD1M03AQ1002158 4RD1M03AQ1002383 4RD1MasAQ1002444 4RD1M03AQ1002561 4RD1M03AQ1002858 4RD1MFVAQ1400233
4RD1M03DPCEVALLO 4RD1M03DSasEGas 4RD1QWDSRAMIREZ 4RD1M03LMARIOS 4RD1M03LNA002885 4RD1WS3LNA002939
4RD1M03LPCRUZ 4RD1M03LPYANEZ 4RD1M03NA002293 4RD1AD7DDCESPEDE 4RD1AD7DMAYJACOM 4RD1AD7DMOVENEGA
4RD1SS4AQ1001901 4RD1AD7AQ1002086 4RD1AD7AQ1002180 4RD1MS04AQ1002185 4RD1AD7AQ1002440 4RD1AD7AQ1002597
4RD1FF4AQ1173294 4RD1AD7AQ1177043 4RD1AD7AQ1400096 4RD1FG4AQ1E43104 4RD1AD7AQ1T03565 4RD1AD7DREUNION
4RD1FF4DSUPTEL01 4RD1AD7DVGAIBOR 4RD1AD7LABARRasA 4RD1AD7LARUBIO 4RD1MWWLHGRIJALV 4RD1AD7LJMARCA
4RD1AD7LMGUasRA 4RD1AD7LMLEON 4RD1M0MWVENEGA 4RD1AD7LNA001506 4RD1AD7LNA002429 4RD1AD7LF002921
4RD1AD7LNA002930 4RD1M0NA002973 4RD1AD7VBA177243 4RD1AD7LNA400351 4RD1AD7LVAPAZMIN 4RD1M0SE·002491
4RD1P0NDMOSORIO 4RD1P0NAQ1000247 4RD1SWSNA002251 4RD1P0NAQ1002275 4RD1P0NAQ1002435 4RD1P0NAQ1002437
4RD1P0NAQ1002491 4RD1P0NAQ1002911 4RD1P0NAQ1002965 4RD1P0NAQ1E00345 4RD1P0NDNPALADIN 4RD1P0NDORLAMUNO
4RD1P0NDRCHasREZ 4RD1P0NDTEMP5RG 4RD1P0NDVBENALCA 4RD1P0NDVCORDOVA 4RD1P0NLCADONOSO 4RD1P0NLIEGas
4RD1P0NLLIPABON 4RD1P0NLMVILLAVI 4RD1P0NLNA001316 4RD1P0NLNA001646 4RD1P0NLNA002024 4RD1P0NLNA002194
4RD1P0NLNA002196 4RD1P0NLNA002401 4RD1P0NLNA186312 4RD1P0NLNA400181 4RD1P0NLOMONJARE 4RD1P0NLYJARAM
4RD1RT9DAGAETE 4RD1RT9DCAMBIO02 4RD1RT9AQ1002277 4RD1RT9AQ1002510 4RD1RT9AQ1002523 4RD1RT9AQ1002568
4RD1RT9AQ1002620 4RD1RT9AQ1002877 4RD1RT9AQ1002915 4RD1RT9AQ1184482 4RD1RT9DPTAPIA 4RD1RT9LCBAQUas
4RD1RT9LMAMORES 4RD1RT9LMARIGAIB 4RD1RT9LNA001339 4RD1RT9LNA001967 4RD1RT9LNA002388 4RD1RT9LNA002467
4RD1RT9LNA002510 4RD1RT9LNA002726 4RD1RT9LNA002759 4RD1RT9LNA002769 4RD1RT9LNA002915 4RD1RT9LNA181913
4RD1RT9LNA186310 4RDDFESPINOS 4RD1JJUDJBOLANO 4RD1JJUDMONITOR 4RD1JJUDPJSAN 4RD1JJUDRBARCENA
4RD1JJULANBORSJA1 4RD1JJULCRILOPEZ 4RD1JJULDORTIZ 4RD1JJULEARIas 4RD1JJULFESPINO2 4RD1JJULHCHAMORR
4RD1JJULHLLasENA 4RD1JJULIORDONEZ 4RD1JJULJBOLANOS 4RD1JJULJCABALLE 4RD1JJULNA002225 4RD1JJULNA002422
4RD1JJULNA002494 4RD1JJULNA002740 4RD1JJULNA002791 4RD1JJULNA002961 4RD1JJULPESPINOS 4RD1JJULPJSANCH
4RD1JJULRBARCENA 4RD1JJULXGARZON 4RD1IOPDGALOPINO 4RD1IOPAQ1400176 4RD1IOPLAGALARZA 4RD1IOPLCMENESES
4RD1IOPLFESPINO1 4RD1IOPLGALOPINO 4RD1IOPLJCORVA 4RD1IOPLJLEON01 4RD1IOPLMIDROVO 4RD1IOPLMSAENZ
4RD1IOPLNA002063 4RD1IOPLNA002273 4RD1IOPLNA184014 4RD1IOPLNA40011 4RD1IOPLRCHECA 4RD1IOPLXLANDAZU
4RD1IOPNA176048 4RD1123DAVasQUEZ 4RD1123AQ1002178 4RD1123LADONOSO 4RD1123LHORDONEZ 4RD1123LNA179879
4RD1123LSCONTRas 4RD1123LVSANTOS 4RD1as0CL183088 4RD1as0DGHasNAND 4RD1as0AQ1002002 4RD1as0AQ1002174
4RD1as0AQ1002375 4RD1as0AQ1002410 4RD1as0AQ1002807 4RD1as0AQ1002958 4RD1as0AQ1002994 4RD1as0AQ1400185
4RD1as0AQ1E48153 4RD1as0AQ1T03647 4RD1as0DNJARAMIL 4RD1as0DPRUEBA01 4RD1as0DPRUEBA02 4RD1as0DPRUEBA03
4RD1as0DVBOADA 4RD1as0LNA002226 4RD1as0LNA002247 4RD1as0LNA002790 4RD1as0LNA400137 4RD1as0LSHasRas
4RD1as0LVGOMEZ 4RD1as0LWSALAZAR 4RD1as1AQ1002280 4RD1as1AQ1002497 4RD1as1AQ1002854 4RD1as1LESALAZAR
4RD1as1LJBEDON 4RD1as1LLGUEVAR 4RD1as1LMRAMIREZ 4RD1as1LNA001447 4RD1as1LNA002482 4RD1as1LNA002936
4RD1as1LNA02497 4RD1as1LNA179051 4RD1as1LNA188658 4RD1as1LPCHICO 4RD1as1LTGONZALE 4RD1as1LXLUZURI
4RD1as2DANCEVALL 4RD1as2AQ1002327 4RD1as2LACOBOS 4RD1as2LAFREIRE 4RD1as2LANAARIZA 4RD1as2LDAMENA
4RD1as2LDELACADE 4RD1as2LDMEND 4RD1as2LasIBADE 4RD1as2LFCISNasO 4RD1as2LGCAMPO 4RD1as2LGHasRasA
4RD1as2LHVIDAL 4RD1as2LJESCOBAR 4RD1as2LNA002025 4RD1as2LNA002038 4RD1as2LNA002059 4RD1as2LNA002061
4RD1as2LNA002068 4RD1as2LNA002331 4RD1as2LNA002486 4RD1as2LNA002501 4RD1as2LNA002512 4RD1as2LNA002519
4RD1as2LNA002754 4RD1as2LNA002840 4RD1as2LNA177893 4RD1as2LSVILLAVI 4RD1as3DCORTIZ 4RD1as3DLREYES
4RD1as3AQ1002044 4RD1as3AQ1002085 4RD1as3AQ1002199 4RD1as3AQ1002893 4RD1as3AQ1184056 4RD1as3DPGUasRA
4RD1as3DTRIVINO 4RD1as3LNA002473 4RD1as3LNA002859 4RD1as3LNA189253 4RD1as4DEZAMBR01 4RD1as4DJGUATO
4RD1as4AQ1002969 4RD1as4LBYHasRas 4RD1as4LDIEVEGA1 4RD1as4LEZAMBRAN 4RD1as4LMIPANCHI 4RD1as4LNA002065
4RD1as4LNA002269 4RD1as4LNA002971 4RD1as4LROZUMB 4RD1as4LSLLININ 4RD1MPBCAV061 4RD1MPBCAVAAL8
4RD1MPBDBODEGA1 4RD1MPBDCABVS11 4RD1MPBDCAV01 4RD1MPBDCAV08 4RD1MPBDCAV098 4RD1MPBDCAV10 4RD1MPBDCAV12
4RD1MPBDCAV14 4RD1MPBDCAV19 4RD1MPBDCAV28 4RD1MPBDCAVDRU 4RD1MPBDCAVS01 4RD1MPBDCAVS3ZTG 4RD1MPBDCAVS4RG1
4RD1MPBDCAVS5CG1 4RD1MPBDCAVSB5B5 4RD1MPBDCAVSFB2Z 4RD1MPBDCAVSREP7 4RD1MPBDCAVSRP2P 4RD1MPBDCONSOLA1
4RD1MPBDCONSOLA9 4RD1MPBDDGUDINO 4RD1MPBDJMARC1 4RD1MPBDKIOSKORP 4RD1MPBDMCHAMORR 4RD1MPBDMFRUIZ55
4RD1MPBDMODUL004 4RD1MPBDMONITORE 4RD1MPBAQ1002245 4RD1MPBAQ1002491 4RD1MPBAQ1002749 4RD1MPBAQ1E0428
4RD1MPBAQ1E04284 4RD1MPBAQ1E04408 4RD1MPBAQ1E04409 4RD1MPBDTOUCH 4RD1P02AQ1002803 4RD1P02AQ1002954
4RD1P02LAESQUIVE 4RD1P02LCCasA 4RD1P02LHUBRAZAL 4RD1P02LJEARIas 4RD1P02LNA002212 4RD1P02LNA002382
4RD1P02LNA002694 4RD1P02LNA002821 4RD1P02LNA400234 4RD1P03DAMALDONA 4RD1P03AQ1001541 4RD1P03AQ1001760
4RD1P03AQ1001999 4RD1P03AQ1002224 4RD1P03AQ1002573 4RD1P03AQ1187689 4RD1P03DPRESTAMO 4RD1P03LCHMORENO
4RD1P03LCIFUENTE 4RD1P03LCMANCILL 4RD1P03LCONATE00 4RD1P03LCTAMAYO 4RD1P03LCTRUJILL 4RD1P03LCVasCONE
4RD1P03LCZHININ 4RD1P03LDELAVEGA 4RD1P03LEAMORES0 4RD1P03LESGALLEG 4RD1P03LFBasTID 4RD1P03LFRPULUPA
4RD1P03LFTOLEDO0 4RD1P03LGAVILA1 4RD1P03LGIRIVasA 4RD1P03LIVITasI 4RD1P03LJGUAITAR 4RD1P03LJPAULIN
4RD1P03LKACAICED 4RD1P03LKSALAZAR 4RD1P03LLVILLAGO 4RD1P03LMALBAN 4RD1P03LMROMO 4RD1P03LNA001331

4RD1P03LNA001845 4RD1P03LNA001999 4RD1P03LNA002015 4RD1P03LNA002016 4RD1P03LNA002017 4RD1P03LNA002021
4RD1P03LNA00215 4RD1P03LNA002224 4RD1P03LNA002298 4RD1P03LNA002339 4RD1P03LNA002342 4RD1P03LNA00244
4RD1P03LNA002500 4RD1P03LNA002514 4RD1P03LNA002516 4RD1P03LNA002715 4RD1P03LNA002799 4RD1P03LNA002802
4RD1P03LNA002871 4RD1P03LNA177171 4RD1P03LNA177732 4RD1P03LNA186435 4RD1P03LNA189211 4RD1P03LNA400090
4RD1P03LNA400120 4RD1P03LNA400209 4RD1P03LNA400216 4RD1P03LOPOLO 4RD1P03LPPAZOS 4RD1P03LRARTEAGA
4RD1P03LRMANTILL 4RD1P03LXCasTILL 4RD1P04AQ1002321 4RD1P04LFFONSECA 4RD1P04LNA001953 4RD1P04LNA002033
4RD1P04LNA002647 4RD1P04LNA002691 4RD1P04LNA178320 4RD1P05DAPAREDES 4RD1P05DFRGUZMAN 4RD1P05AQ1002040
4RD1P05AQ1002445 4RD1P05AQ1002727 4RD1P05AQ1002913 4RD1P05AQ1002914 4RD1P05AQ1002916 4RD1P05AQ1002922
4RD1P05AQ1002924 4RD1P05AQ1177641 4RD1P05AQ1187687 4RD1P05DPRUEBas 4RD1P05DSBENITEZ 4RD1P05ENA002548
4RD1P05LAGUasRON 4RD1P05LCIREYES 4RD1P05LDCADENA0 4RD1P05LDCAMINO 4RD1P05LEAREVALO 4RD1P05LEMasA123
4RD1P05LEMINO001 4RD1P05LasIANDRA 4RD1P05LGHINOJO 4RD1P05LGHINOJOS 4RD1P05LGURIBE 4RD1P05LHFREIRE
4RD1P05LJCasTRO 4RD1P05LJLOAIZA 4RD1P05LJVILLACR 4RD1P05LLCARLOSA 4RD1P05LMCCHAVEZ 4RD1P05LN002345
4RD1P05LNA001950 4RD1P05LNA002010 4RD1P05LNA002036 4RD1P05LNA002255 4RD1P05LNA002301 4RD1P05LNA002346
4RD1P05LNA002405 4RD1P05LNA002478 4RD1P05LNA002483 4RD1P05LNA002502 4RD1P05LNA002510 4RD1P05LNA002548
4RD1P05LNA002613 4RD1P05LNA002875 4RD1P05LNA002916 4RD1P05LNA002995 4RD1P05LNA400248 4RD1P05LPasANTE1
4RD1P05LRBARBA 4RD1P05LROSALAZA 4RD1P05LWCHUQUI 4RD1P05LXORTIZ 4RD1P05NA002890 4RD1P06D4CP5RG1
4RD1P06DasAMANIE 4RD1P06DCAPA4RG1 4RD1P06DCAPA5RG1 4RD1P06DCAVS03 4RD1P06DCCENTas3 4RD1P06DCCENTas4
4RD1P06DDSALVADO 4RD1P06DEESPINOS 4RD1P06DESALAZAR 4RD1P06DFVALLEJO 4RD1P06DGSANCHEZ 4RD1P06DHYANEZ
4RD1P06DJPACHECO 4RD1P06DKRIVADE 4RD1P06DMAGUZMAN 4RD1P06DMARROYO 4RD1P06DMBONILLA 4RD1P06DMJALIL
4RD1P06DN002320 4RD1P06AQ1000132 4RD1P06AQ1001665 4RD1P06AQ1001939 4RD1P06AQ1002011 4RD1P06AQ1002101
4RD1P06AQ1002113 4RD1P06AQ1002120 4RD1P06AQ1002167 4RD1P06AQ1002175 4RD1P06AQ1002195 4RD1P06AQ1002197
4RD1P06AQ1002210 4RD1P06AQ1002211 4RD1P06AQ1002219 4RD1P06AQ1002227 4RD1P06AQ1002234 4RD1P06AQ1002281
4RD1P06AQ1002285 4RD1P06AQ1002294 4RD1P06AQ1002380 4RD1P06AQ1002394 4RD1P06AQ1002449 4RD1P06AQ1002469
4RD1P06AQ1002493 4RD1P06AQ1002518 4RD1P06AQ1002575 4RD1P06AQ1002605 4RD1P06AQ1002620 4RD1P06AQ1002714
4RD1P06AQ1002721 4RD1P06AQ1002776 4RD1P06AQ1002801 4RD1P06AQ1002847 4RD1P06AQ1002863 4RD1P06AQ1002864
4RD1P06AQ1002870 4RD1P06AQ1002886 4RD1P06AQ1002912 4RD1P06AQ1002918 4RD1P06AQ1002925 4RD1P06AQ1002943
4RD1P06AQ1002957 4RD1P06AQ1182491 4RD1P06AQ1184482 4RD1P06AQ1186315 4RD1P06AQ1187044 4RD1P06AQ1187688
4RD1P06AQ1400070 4RD1P06AQ1400118 4RD1P06AQ1400121 4RD1P06AQ1400126 4RD1P06AQ1400128 4RD1P06AQ1400129
4RD1P06AQ1400215 4RD1P06DPAGUEVAR 4RD1P06DPCRUZ002 4RD1P06DRHasEDIA 4RD1P06DSAGUIR 4RD1P06DSCORVA
4RD1P06DVBARRENO 4RD1P06DXMOLINA 4RD1P06DXPONCE 4RD1P06LACGARCIA 4RD1P06LACHILUIS 4RD1P06LCMOLINA
4RD1P06LFVALLEJO 4RD1P06LHPINCAY 4RD1P06LJOLEas 4RD1P06LMCOSTA 4RD1P06LMTFLORES 4RD1P06LNA000321
4RD1P06LNA002000 4RD1P06LNA002004 4RD1P06LNA002172 4RD1P06LNA002262 4RD1P06LNA002284 4RD1P06LNA002286
4RD1P06LNA002304 4RD1P06LNA00294 4RD1P06LNA002955 4RD1P06LNA002992 4RD1P06LNA002996 4RD1P06LNA002997
4RD1P06LNA400210 4RD1P06LVGALLEGO 4RD1P06LWMIN 4RD1P06NA002213 4RD1P06NA002965 4RD1P07DACORRAL
4RD1P07DAMARIA 4RD1P07DMAYGUA 4RD1P07AQ100131 4RD1P07AQ1002102 4RD1P07AQ1002164 4RD1P07AQ1002283
4RD1P07AQ1002346 4RD1P07AQ1002385 4RD1P07AQ1002420 4RD1P07AQ1002563 4RD1P07AQ1002588 4RD1P07AQ1002592
4RD1P07AQ1002663 4RD1P07AQ1002741 4RD1P07AQ1002742 4RD1P07AQ1002868 4RD1P07AQ1002891 4RD1P07AQ1002919
4RD1P07AQ1177641 4RD1P07AQ1177737 4RD1P07AQ1180205 4RD1P07AQ1181973 4RD1P07AQ1182819 4RD1P07AQ1186628
4RD1P07AQ1400051 4RD1P07AQ1400111 4RD1P07AQ1400139 4RD1P07DPPasEZ 4RD1P07LDPROANO 4RD1P07LEDONOSO
4RD1P07LasACINES 4RD1P07LFRBasTID 4RD1P07LGCasTRO 4RD1P07LKCARDENA 4RD1P07LMFCALDas 4RD1P07LN186627
4RD1P07LNA001456 4RD1P07LNA002120 4RD1P07LNA002146 4RD1P07LNA002164 4RD1P07LNA002190 4RD1P07LNA002239
4RD1P07LNA002259 4RD1P07LNA002272 4RD1P07LNA002302 4RD1P07LNA002317 4RD1P07LNA002658 4RD1P07LNA002665
4RD1P07LNA002707 4RD1P07LNA002761 4RD1P07LNA002850 4RD1P07LNA002891 4RD1P07LNA002952 4RD1P07LNA002972
4RD1P07LNA179623 4RD1P07LNA183090 4RD1P07LROHasEDI 4RD1P07LVESTUP11 4RD1P07LVILLACIS 4RD1P07MELOPEZ
4RD1P07NA002152 4RD1P07PSALACOM 4RD1P08LNA001272 4RD1P08LNA002267 4RD1P08LNA002577 4RD1P08LNA002715
4RD1P08LNA002962 4RD1P090000DARON 4RD1P09DABALDEON 4RD1P09DALEJACOS 4RD1P09DANPAUCA 4RD1P09DAPTORRES
4RD1P09DCUADROFA 4RD1P09DDESALas 4RD1P09DGDAVILA 4RD1P09DGVALENZU 4RD1P09DHVasCONE 4RD1P09DMAVALLAD
4RD1P09DMRUIZ 4RD1P09DMSANTA 4RD1P09AQ1000471 4RD1P09AQ1002034 4RD1P09AQ1002176 4RD1P09AQ1002184
4RD1P09AQ1002246 4RD1P09AQ1002270 4RD1P09AQ1002278 4RD1P09AQ1002316 4RD1P09AQ1002341 4RD1P09AQ1002355
4RD1P09AQ1002444 4RD1P09AQ1002488 4RD1P09AQ1002572 4RD1P09AQ1002670 4RD1P09AQ1002709 4RD1P09AQ1002756
4RD1P09AQ1002775 4RD1P09AQ1002856 4RD1P09AQ1002876 4RD1P09AQ1002878 4RD1P09AQ1002934 4RD1P09AQ102964
4RD1P09AQ1176993 4RD1P09AQ1184485 4RD1P09AQ1400140 4RD1P09AQ1E46707 4RD1P09AQ1IORTIZ 4RD1P09DPMENA
4RD1P09DYJATIVA 4RD1P09LAMONGE 4RD1P09LCVITasI1 4RD1P09LDAMOREAN 4RD1P09LDCORTIZP 4RD1P09LFALVARAD
4RD1P09LGOROZCO 4RD1P09LLUEGA 4RD1P09LMAMARTIN 4RD1P09LMFHIDALG 4RD1P09LMTUQUas1 4RD1P09LMVILLEGA
4RD1P09LN4002968 4RD1P09LNA001204 4RD1P09LNA002018 4RD1P09LNA00203 4RD1P09LNA00207 4RD1P09LNA002181
4RD1P09LNA002191 4RD1P09LNA002215 4RD1P09LNA002456 4RD1P09LNA002484 4RD1P09LNA002539 4RD1P09LNA002669
4RD1P09LNA002725 4RD1P09LNA002767 4RD1P09LNA002798 4RD1P09LNA002809 4RD1P09LNA002920 4RD1P09LNA002934
4RD1P09LNA002964 4RD1P09LNA002968 4RD1P09LNA002971 4RD1P09LNA002986 4RD1P09LNA183679 4RD1P09LNA400226
4RD1P09LNP183682 4RD1P09LRESCOBAR 4RD1P09LROENDARA 4RD1P09LWMALDONA 4RD1P09LWSUAREZ1 4RD1P09LXAHasRas
4RD1P10DCAPAZTG5 4RD1P10DEFREIRE 4RD1P10DINTasA08 4RD1P10AQ1E04307 4RD1P10AQ1E04341 4RD1P10LNA176285
4RD1P12AQ1002879 4RD1P12AQ1182589 4RD1P12AQ1184484 4RD1P12LGVasQZ01 4RD1PMZAQ151101 4RD1PMZAQ1E50338
4RD1PMZAQ1E51100 4RD1PMZAQ1E51102 4RD1PMZAQ1E51204 4RD1PMZAQ1T03566 4RD1PMZAQ1T03599 4RD1PMZAQ1T03603
4RD1PMZAQ1T3570 4RD1PMZLEDVILLAC 4RD1PMZLJANDRADE 4RD1PMZLMFYEPEZ 4RD1PMZLNA002216 4RD1PMZLNA002387
4RD1PMZLNA503569 4RD1PMZLNAE03567 4RD1PMZLNAT03570 4RD1PMZLPEMEDINA 4RD1QN1CAVS00026 4RD1QN1DCAVS0002
4RD1QN1DCAVS0003 4RD1QN1DCAVS0004 4RD1QN1DCAVS0006 4RD1QN1DCAVS0007 4RD1QN1DCAVS0008 4RD1QN1DCAVS0009
4RD1QN1DCAVS0010 4RD1QN1DCAVS0011 4RD1QN1DCAVS0012 4RD1QN1DCAVS0013 4RD1QN1DCAVS0016 4RD1QN1DCAVS0017
4RD1QN1DCAVS0030 4RD1QN1DCAVS005 4RD1QN1DCAVSCOT1 4RD1QN1DCAVSCOT2 4RD1QN1DKIOSKO 4RD1X01DDFasNAN
4RD1X01DMACasO 4RD1X01AQ1002974 4RD1X01AQ1189078 4RD1X01LAREINOSO 4RD1X01LCALME 4RD1X01LDIPINTO
4RD1X01LDMENA 4RD1X01LEDALMEID 4RD1X01LGGUasRas 4RD1X01LHasGUasR 4RD1X01LJFLORES 4RD1X01LJMARQUEZ
4RD1X01LJSANTOS 4RD1X01LKZURITA 4RD1X01LMAJACOas 4RD1X01LMROSasO 4RD1X01LMVILLAMA 4RD1X01LNA001103
4RD1X01LNA001330 4RD1X01LNA001673 4RD1X01LNA001995 4RD1X01LNA002030 4RD1X01LNA002183 4RD1X01LNA002188

4RD1X01LNA002190 4RD1X01LNA002332 4RD1X01LNA02610 4RD1X01LNA183020 4RD1X01LNA400182 4RD1X01LNA400189 4RD1X01LNA400194 4RD1X01LPBRAV012 4RD1X01LTAEASDVE 4RD1X01LVEZXCV12 4RD1X01LZCDas 4RD1X02AQ1000458 4RD1X02AQ1001657 4RD1X02AQ1002289 4RD1X02AQ1002808 4RD1X02DPAZXI 4RD1X02DPAPCXZX 4RD1X02LAASDCXVBREZ 4RD1X02LABAASDZA 4RD1X02LANNASDFAJ 4RD1X02LAZADSUMB 4RD1X02ZMCCZ 4RD1X02LDIDALG 4RD1X02LDASDASDVAD 4RD1X02LEXCRA 4RD1X02LFasAS23 4RD1X02LRASDFES 4RD1X0OZXCVZXC 4RD1X02LJGMINO 4RD1X02LSDRIAG 4RD1X02DSasO 4RD1X02LMFR324S 4RD1X02LMSasXCV123 4RD1X02LNA000459 4RD1X02LNA000642 4RD1X02LNA001207 4RD1X02LNA001454 4RD1X02LNA001562 4RD1X02LNA001575 4RD1X02LNA001620 4RD1X02LNA001713 4RD1X02LNA001808 4RD1X02LNA001945 4RD1X02LNA002008 4RD1X02LNA002035 4RD1X02LNA002287 4RD1X02LNA002398 4RD1X0ASDA002409 4RD1X02LNA002518 4RD1X02LNA002564 4RD1X02LNA002585 4RD1X02LNA002760 4RD1X02LNA002800 4RD1X02LA00ASD2806 4RD1X02LNA002867 4RD1X02LNA002878 4RD1X02LNA002880 4RD1X02LNA002888 4RD1X02LNA101562 4RD1X02LNA4ASD06 4RD1X02LNA400256 4RD1X02LPAGO234S 4RD1X02LPA234BAN 4RD1X02LPAPROANO 4RD1X02LPSANTILL 4RD1X02LSDARAM 4RD1X02LSCABZDasA 4RD1X02LSMDWE 4RD1X02LSPAD234LA 4RD1X02LSPAILIAC 4RD1X02VO34234EZ 4RD1XPBD002316 4RD1XPBD CXVZXCVREA 4RD1XPBAQ1000247 4RD1XPBAQ1000430 4RD1XPBAQ1001611 4RD1XPBAQ1002134 4RD1XPBAQ1002268 4RD1XPBAQ1002359 4RD1XPBAQ1400048 4RD1XPBAQ1E43689 4RD1XPBAQ1T03586 4RD1XPBDSO234VIL 4RD1XPBDV345ANO 4RD1XPBEZXCRGA 4RD1XPBLDMARTINE 4RD1XPBLFSOJOS12 4RD1XPBLJARQUE 4RD1XPBLMAL57645 4RD1XPBLNA001491 4RD1XPBLNA002150 4RD1XPBLNA002433 4RD1XPBLNA002471 4RD1XPBLNA002584 4RD1XPBLNA002616 4RD1XPBLNA002705 4RD1XPBLNA181304 4RD1XPBLVBRAVO 4RD1XPBLVTUPIN 4RD1XPBMAUNA 4RD1XPBMLHIDALG 4RD1XPBNA001791 4RD1XPBNA002607 WEBPOP01 WSECUVM01 WSECUVM02 WSECUVM03 CNU315BYR0 CND1100Z69 CNU2409CLF CND1100V1Z 3HJ75K1 CNASDD1100TSM FH3NRG1 CND11010Z4 CNU1170W1L 6H3NRG1 BQ8VRG1 CND11013LS 8V8VRG1 CNU2409CQ1 CND0351J54 CND11ASD00TSM CNU2419JDP CND1100ZS4 CND11110148Q MXL2392FYH 6FP5RG1 MXL2490V0X 70D7RG1 MXL2392FYM JLQ1VG1 95D7RG1 GGPAS5RG1 SEASRIE BAAN02CG1 9ASDCF2CG1 CX02CG1 5Z3ZTG1 CNU315BX9J 2CE3102H4D CNU2419JF0 CND1110XT CND1100TYY CND1100TNC CND1100TXV 2CE3102H89 CND1100V2P CNU21919HM

En resumen, esta familia de protocolos dentro de la red, debería ser revisada y securizada convenientemente. En realidad la máxima ocurrencia de este tipo de tráfico <u>se debe a hosts configurados por defecto</u>, es decir la instalación de Windows nativa que no fue securizada (bastionada o hardening) por lo tanto genera este tipo de tráfico innecesario y que como acabamos de ver ofrece información muy valiosa para cualquier intruso.

A continuación se presentan algunas capturas más de estos tipos de tráfico:

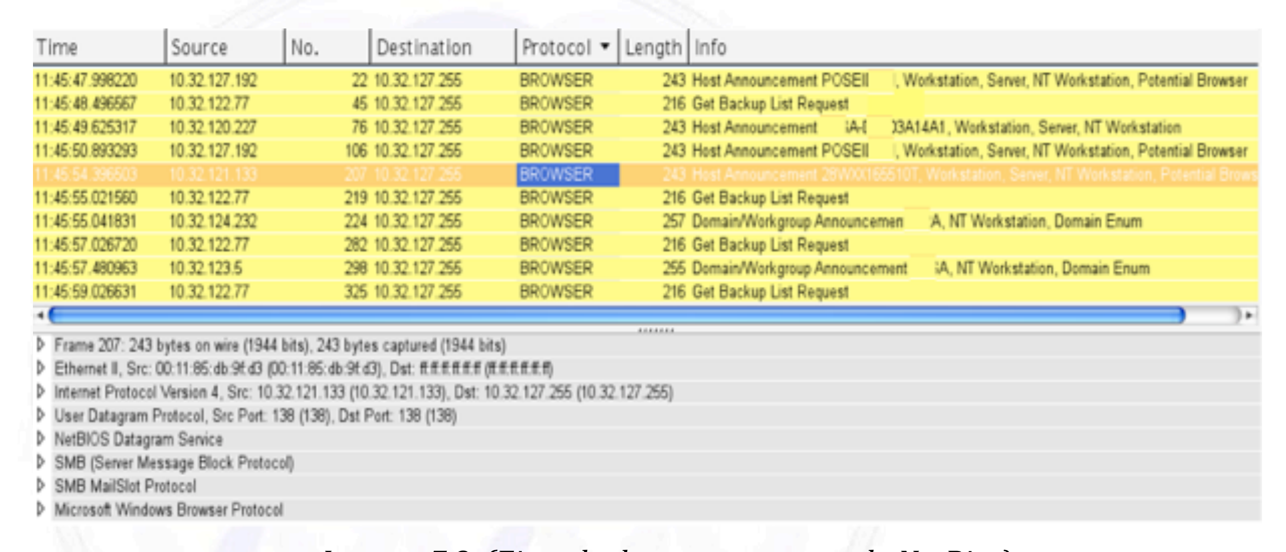


Imagen 7.8 (Ejemplo de captura protocolo NetBios)

Time	Source	No.	Destination	Protocol	Length	Info
11:45:47.250177	10.32.121.125	8	10.32.127.255	NBNS	92	Name query NB 28NE 22.TC <54>
11:45:47.359629	10.32.121.125	11	10.32.127.255	NBNS	92	Name query NB 28NE 20.T0. <54>
11:45:47.422765	10.32.127.223	13	10.32.127.255	NBNS	92	Name query NB HP79F <00>
11:45:47.604218	10.32.121.115	17	10.32.127.255	NBNS	92	Name query NB WPAD.T0.I <00>
11:45:47.799332	10.32.120.193	18	10.32.127.255	NBNS	92	Name query NB T148317.T0.I <00>
11:45:48.109727	10.32.121.125	25	10.32.127.255	NBNS	92	Name query NB 28NE 20.T0.INE<54>
11:45:48.172974	10.32.127.223	27	10.32.127.255	NBNS	92	Name query NB HP79F <00>
11:45:48.313411	10.32.120.221	28	10.32.127.255	NBNS	92	Name query NB 28NBRD18.T0 <54>
11:45:48.354324	10.32.121.115	31	10.32.127.255	NBNS	92	Name query NB WPAD.T0.I <00>
11:45:48.508643	10.32.122.77	50	10.32.127.255	NBNS	92	Name query NB BLI<1b>

- Frame 106: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
- Ethernet II, Src: 00:08:74:aa:09:1d (00:08:74:aa:09:1d), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 10.32.127.192 (10.32.127.192), Dst: 10.32.127.255 (10.32.127.255)
- User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
- NetBIOS Datagram Service
- SMB (Server Message Block Protocol)
- SMB MailSlot Protocol
- Microsoft Windows Browser Protocol

Imagen 7.9 (Ejemplo de captura protocolo NetBios)

7.6. CDP (Cisco Discovery Protocol)

Este es uno de los protocolos primarios de Cisco que facilita el funcionamiento de sus dispositivos para ser configurados vía Broadcast, cosa que actualmente es muy poco probable que se emplee en grandes redes y de la información que hemos podido recolectar en las diferentes redes con las que hemos trabajado, no se está empleando para esta función, por lo tanto no tiene sentido que esté activo y generando tráfico en la red.

Este protocolo, ofrece gran cantidad de información a cualquiera que esté "escuchando" en esa red, y como bien sabemos es innecesario ofrecerla. Debería configurarse '*no cdp run*' .

A continuación presentamos un fragmento de una captura de tráfico realizada en esta red, si se despliega la misma se puede apreciar el tipo y calidad de la información que se difunde innecesariamente, se presentan algunas evidencias de ello:



Imagen 7.10 (Ejemplo de captura protocolo CDP)

A continuación se presenta el detalle de una trama con protocolo CDP capturada en una red, de todos estos campos se puede obtener información muy valiosa para lo que se denomina "Fingerprinting" o "Footpronting" que son las fases preparatorias para el análisis y la intrusión de redes y sistemas:

```
      No.      Time              Source                  Destination             Protocol Length
Info
         1307  00:10:20.685246  00:23:33:08:8f:12       01:00:0c:cc:cc:cc       CDP         424
Device ID: Ej_800.ejemplo.com  Port ID: FastEthernet1/0/16

      Frame 1307: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits)
       IEEE 802.3 Ethernet
          Destination: 01:00:0c:cc:cc:cc (01:00:0c:cc:cc:cc)
          Source: 00:23:33:08:8f:12 (00:23:33:08:8f:12)
          Length: 410
      Logical-Link Control
       Cisco Discovery Protocol
          Version: 2
          TTL: 180 seconds
          Checksum: 0x776e [correct]
              [Good: True]
              [Bad: False]
          Device ID: Ej_800.ejemplo.com
              Type: Device ID (0x0001)
              Length: 34
              Device ID: Ej_800.ejemplo.com
          Software Version
              Type: Software version (0x0005)
              Length: 189
              Software  Version:  Cisco  IOS  Software,  C3750  Software  (C3750-IPBasEK9-M),
Version 12.2(50)SE1, RELEasE SOFTWARE (fc2)
                                Copyright (c) 1986-2009 by Cisco Systems, Inc.
                                Compiled Mon 06-Apr-09 08:19 by ace
          Platform: cisco WS-C3750-24TS
              Type: Platform (0x0006)
              Length: 23
              Platform: cisco WS-C3750-24TS
          Addresses
              Type: Addresses (0x0002)
              Length: 17
              Number of addresses: 1
              IP address: 10.16.25.23
                  Protocol type: NLPID
                  Protocol length: 1
                  Protocol: IP
                  Address length: 4
                  IP address: 10.16.25.23
          Port ID: FastEthernet1/0/16
              Type: Port ID (0x0003)
              Length: 22
              Sent through Interface: FastEthernet1/0/16
          Capabilities
              Type: Capabilities (0x0004)
              Length: 8
              Capabilities: 0x00000028
                  .... .... .... .... .... .... .... ...0 = Not a Router
                  .... .... .... .... .... .... .... ..0. = Not a Transparent Bridge
```




```
                .... .... .... .... .... .... .... .0.. = Not a Source Route Bridge
                .... .... .... .... .... .... .... 1... = Is  a Switch
                .... .... .... .... .... .... ...0 .... = Not a Host
                .... .... .... .... .... .... ..1. .... = Is  IGMP capable
                .... .... .... .... .... .... .0.. .... = Not a Repeater
        Protocol Hello: Cluster Management
            Type: Protocol Hello (0x0008)
            Length: 36
            OUI: 0x00000C (Cisco)
            Protocol ID: 0x0112 (Cluster Management)
            Cluster Master IP: 0.0.0.0
            UNKNOWN (IP?): 0xFFFFFFFF (255.255.255.255)
            Version?: 0x01
            Sub Version?: 0x02
            Status?: 0x21
            UNKNOWN: 0xFF
            Cluster Commander MAC: 00:00:00:00:00:00
            Switch's MAC: 00:23:34:08:8f:00
            UNKNOWN: 0xFF
            Management VLAN: 0
        VTP Management Domain: Bxxxxxx
            Type: VTP Management Domain (0x0009)
            Length: 15
            VTP Management Domain: Bxxxxxx
        Native VLAN: 12
            Type: Native VLAN (0x000a)
            Length: 6
            Native VLAN: 12
        Duplex: Full
            Type: Duplex (0x000b)
            Length: 5
            Duplex: Full
        Trust Bitmap: 0x00
            Type: Trust Bitmap (0x0012)
            Length: 5
            Trust Bitmap: 00
        Untrusted port CoS: 0x00
            Type: Untrusted Port CoS (0x0013)
            Length: 5
            Untrusted port CoS: 00
        Management Addresses
            Type: Management Address (0x0016)
            Length: 17
            Number of addresses: 1
            IP address: 10.16.25.23
                Protocol type: NLPID
                Protocol length: 1
                Protocol: IP
                Address length: 4
                IP address: 10.16.25.23
        Power Available: 0 mW, 4294967295 mW,
            Type: Power Available (0x001a)
            Length: 16
            Request-ID: 0
            Management-ID: 1
            Power Available: 0 mW
            Power Available: 4294967295 mW
```

Como se puede apreciar en la captura de la trama anterior, se presenta en texto plano, Interfaces, direccionamiento, nombre, dominio, modelo de router, versión de

sistema operativo, fecha de compilación, usuario que, lo compiló, etc. Todos estos datos para un intruso tienen mucho valor.

7.7. SSH en su versión 1 (Secure SHell versión 1)

El empleo de la versión 1 de este protocolo, si bien puede ser considerado como un aspecto secundario, debería al menos ya estar considerándose en su migración hacia la versión 2 ya que en la mayoría de las listas de vulnerabilidades el empleo de la versión anterior la catalogan como vulnerabilidad "MEDIA" y esto se debe a que ya se conocen numerosos "exploits" que sin mayor dificultad pueden acceder al dispositivo.

Para que podamos valorar la necesidad de su empleo o no en nuestras redes, a continuación presentamos una tabla con las mayores diferencias entre ambas versiones:

SSH Versión 2	**SSH Versión 1**
separa los protocolos de autenticación y conexión.	es un protocolo monolítico.
robustos algoritmos de chequeo de integridad criptográfica.	débil chequeo de CRC 32 (ya se conoce la posibilidad de ataque de inserción).
soporta cambio de password.	N/A
admite cualquier número de canales por conexión.	exactamente un canal por conexión.
negociación completa de criptografía y algoritmos de compresión modulares, incluyendo cifrado masivo, MAC y clave pública.	negocia sólo el cifrado en bloque.
cifrado y compresión son negociados por separado para cada dirección, con claves independientes.	los mismos algoritmos y claves se utilizan en ambas direcciones (aunque RC4 utiliza claves separadas).
esquema extensible de algoritmo / nombres de protocolo permitiendo extensiones locales, preservando la interoperatibilidad.	codificación fija que impide adiciones de interoperatibilidad.
Métodos de autenticación de usuarios soportados: • Clave pública (con algoritmos: DSA, RSA *sólo en algunas implantaciones*, OpenPGP) • basados en hash • password • rhosts descartado por ser inseguro	Métodos de autenticación de usuarios soportados: • Clave pública (solo RSA) • rhostRSA • rhost(rsh) • password • kerberos
la negociación de claves Diffie-Hellman elimina la necesidad de un servidor de claves.	el servidor de claves es necesario para encaminar el secreto en la generación de la clave de sesión.

soporta certificados digitales	N/A
el intercambio de autenticación de usuarios es más flexible y permite que requiere múltiples formas de autentica-ción para el acceso.	permite exactamente una forma de autenticación por sesión.
la autenticación basada en host es, en principio independiente de la dirección de red del cliente, por lo que le permite trabajar con proxies, clientes móviles, etc.	la autenticación vía rhostsRSA está ligada directamente a la dirección de host del cliente, lo que limita su utilidad.
reemplazo periódico de las claves de sesión	N/A

Un método de presentar esta diferencia es a través de una captura de tráfico.

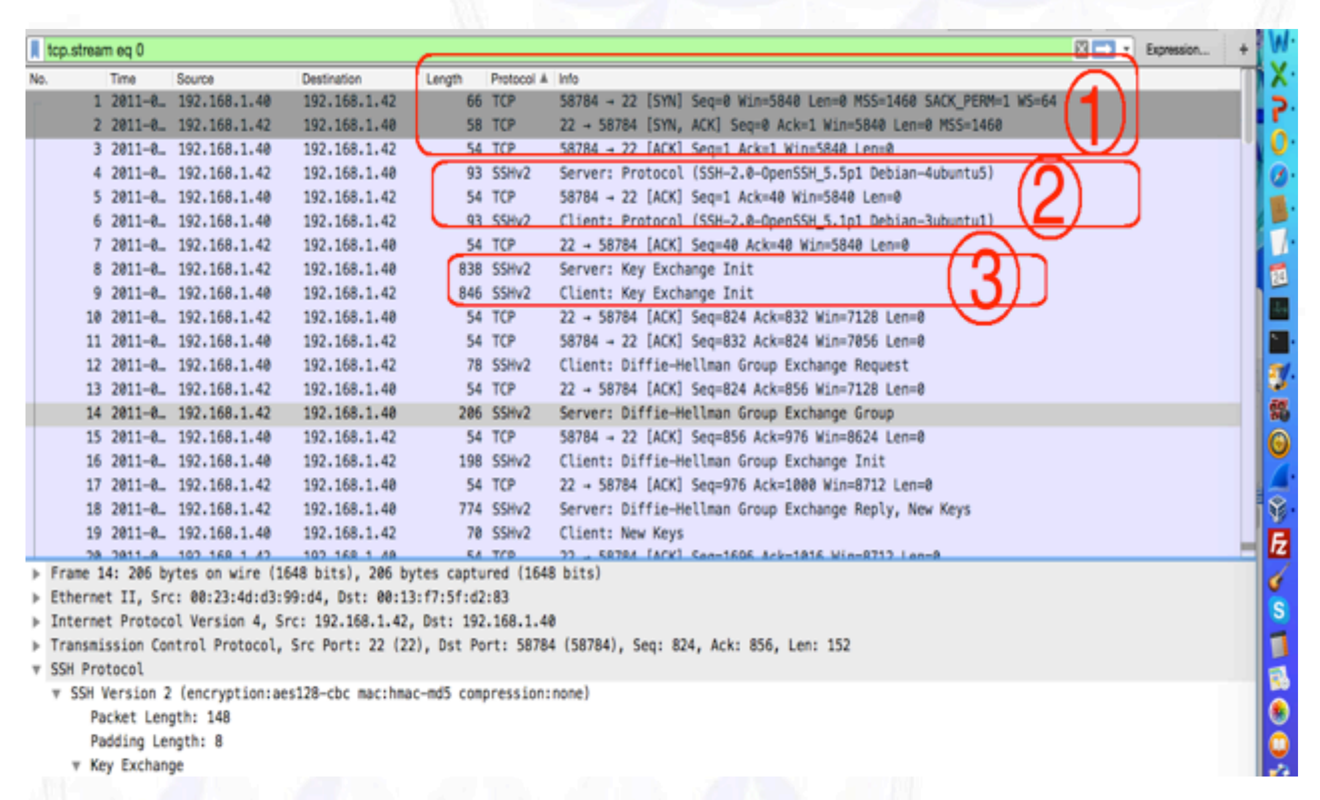


Imagen 7.11 (Ejemplo de captura protocolo SSH versión2)

En la imagen de la captura de arriba, hemos remarcado tres áreas en rojo, la primera **(1)** son las tres tramas que ejecutan el triple handshake sobre el puerto 22, podemos ver el [SYN], el [SYN-ACK] y finalmente el [ACK] con el que queda establecida la sesión TCP sobre el puerto 22, a partir de esta tercer trama, al estar establecida la sesión sobre este puerto, el diálogo ya comienza a ser por medio del nivel "aplicación" a través del protocolo SSH que podemos ver que se trata de la versión 2 del mismo. La segunda área que hemos marcado **(2)** es cuando se hacen presentes entre sí el

servidor y el cliente, y finalmente está el área **(3)** en la cual, se indican todos los protocolos de autenticación que soporta cada uno de ellos.

En la imagen de abajo, hemos realizado el seguimiento de todo este flujo, y se ve con más detalle (*en la ventana emergente que se ve por debajo de la secuencia de tramas de Wireshark*) todos los protocolos y versiones que podrían dialogar en este proceso de autenticación. Esta es justamente una de las grandes diferencias que pusimos de manifiesto en la tabla comparativa entre la versión 1 y la 2.

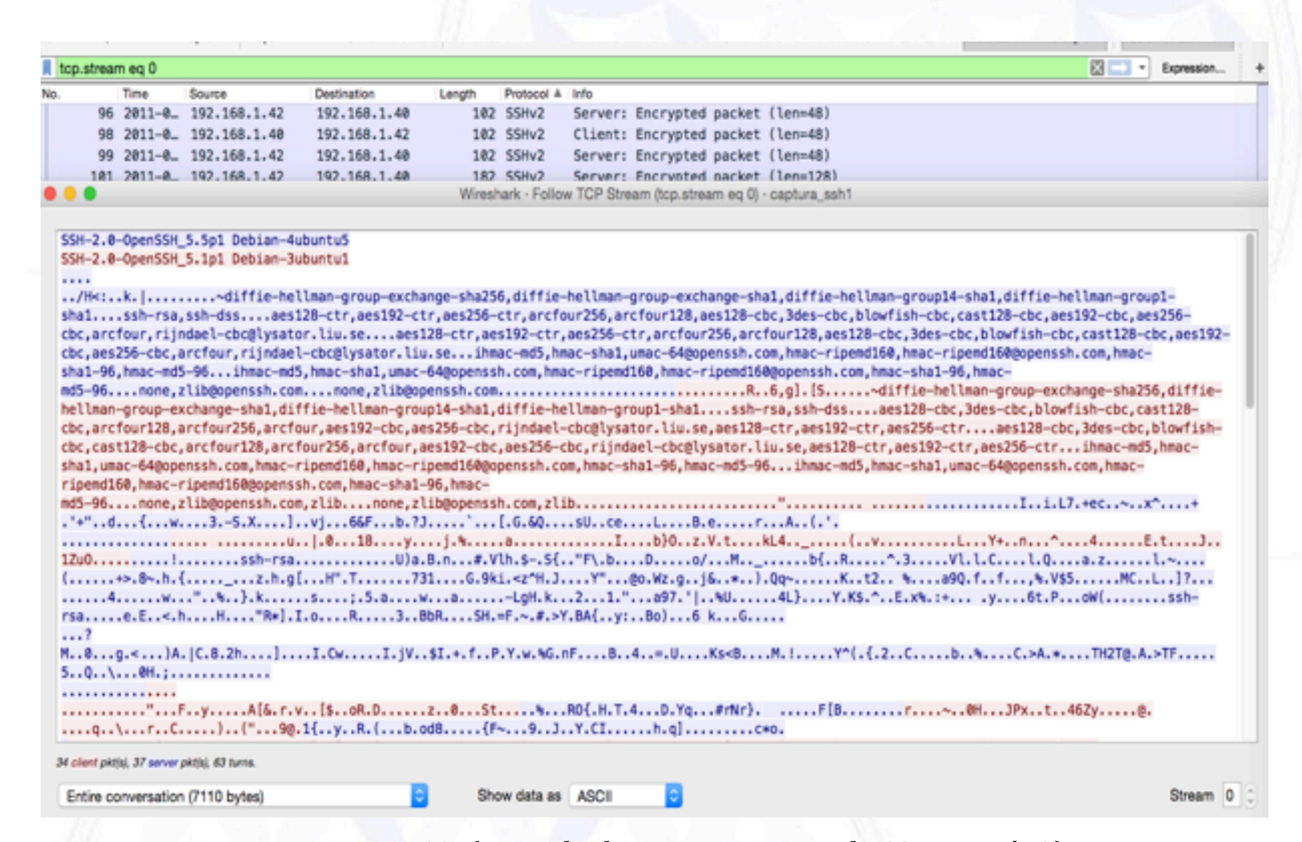


Imagen 7.12 (Ejemplo de captura protocolo SSH versión2)

7.8. HTTP en vez de HTTPS

Dentro de los protocolos cuya información viaja en texto plano, también se encuentra **http**. Este protocolo es de uso frecuente en interfaces gráficas de administración, las cuáles hoy en día admiten TODAS el empleo de **https**, que debería ser la norma. El caso de no poder emplear este último es la excepción, y como siempre se debe documentar y justificar este caso concreto.

A continuación presentamos la imagen de una captura de protocolo http, en la cual hemos consultado un servidor Web sobre el que habíamos escrito el texto: "**esto**

es una prueba de archivo por http" y este mensaje se ve que aparece en texto plano en la captura, también vemos que se aprecia toda la configuración del servidor, la ruta hasta este directorio, etc.. Hemos querido demostrar con este simple ejemplo cómo ofrece información de alto impacto a cualquiera que la escuche.

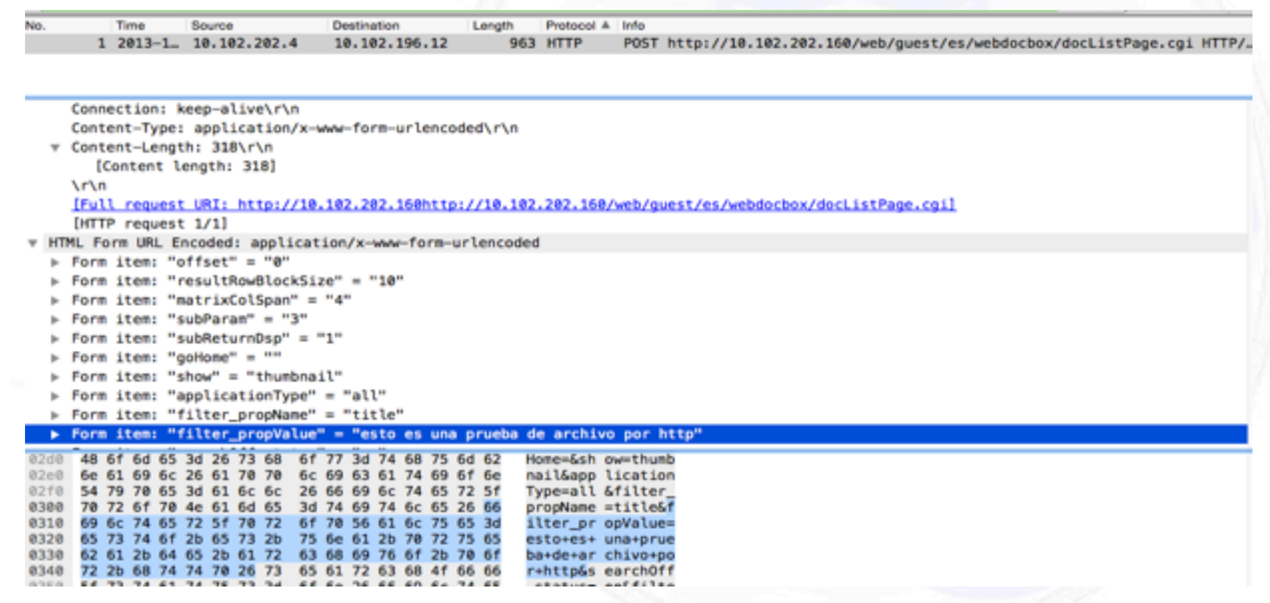


Imagen 7.13 (Ejemplo de captura protocolo http)

Si este mismo tipo de tráfico lo realizamos a través de https (SSL o TLS, que es el nombre estándar para esta familia de protocolo) podemos apreciar en la imagen que sigue que los datos viajan totalmente criptografiados.

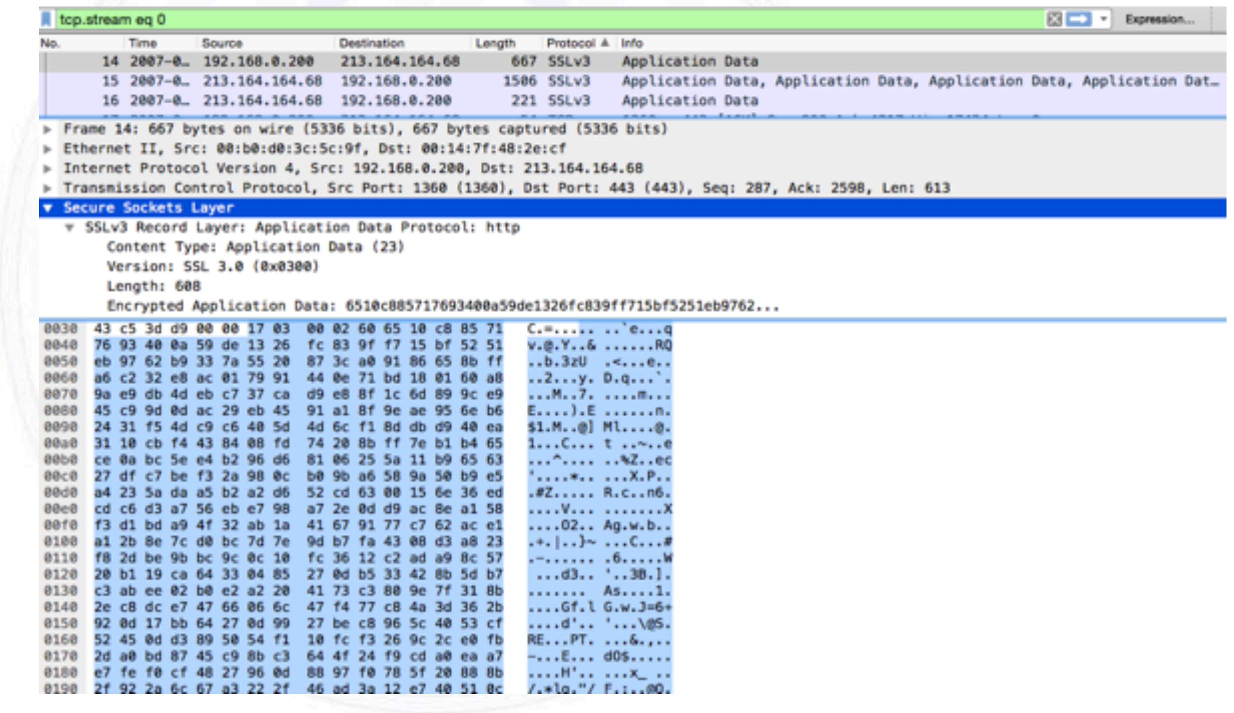


Imagen 7.14 (Ejemplo de captura protocolo https)

7.9. Ausencia de tunelización (donde corresponda).

Hemos presentado ya varios conceptos sobre túneles, lo más importante con lo que nos debemos quedar al respecto es la comparación pura y dura con un túnel de coches o de tren, este tipo de túneles tiene dos características claras:

- Posee una entrada y una salida (únicas).
- Desde dentro del túnel no se ve hacia fuera, y desde fuera no se ve hacia dentro.



Imagen 7.15 (Ejemplo de túnel real)

Si no olvidamos estos dos conceptos, seremos expertos en túneles. La razón fundamental de su implementación son sólo estas dos ideas, luego puede tener varias características que le dan valor agregado, pero su razón de ser son esos dos conceptos.

Por ello es que cuando se analiza un determinado segmento de red, dentro del mismo vínculo físico, seguramente estén viajando más de un tipo de datos, o paquetes de diferentes orígenes, destinos propietarios, tipos de información, etc. En algunos de estos segmentos, estas diferencias no revistan importancia, pero en otros sí, y desde el punto de vista de seguridad, no pueden ser dejadas de lado.

Para profundizar sobre este tema, en la actualidad el mejor ejemplo lo debemos tomar de la familia IPSec sobre la cual encontraremos todo el detalle en el libro "**Seguridad por Niveles**".

Más adelante realizaremos bastantes ejercicios prácticos sobre el empleo de túneles.

7.10. Cómo detectar, analizar y recolectar evidencias de estos protocolos inseguros.

En este punto, nos referimos a la parte práctica de los puntos últimos que hemos desarrollado. En el caso de los protocolos inseguros, las dos fuentes nativas para analizarlos son:

- La configuración de cada nodo.
- La escucha de tráfico.

Necesitamos realizar ambas actividades pues no necesariamente estará circulando ese protocolo débil que buscamos en el momento exacto en el que lanzamos nuestra herramienta, sin embargo sí o sí deberá estar configurado en el elemento de red correspondiente, aunque puede suceder también que justamente los elementos de red sobre los que analicemos su configuración estén adecuadamente configurados, pero otros no, en esos casos es cuando podemos llegar a localizarlos con escuchas de tráfico. En la parte de ejercitaciones, veremos cómo se puede dejar configurada una sonda para escuchar únicamente un determinado patrón de tráfico, y que no capture el resto, con este tipo de escuchas, puede quedar nuestra sonda conectada a ese segmento, y únicamente capturará el tráfico que estamos buscando, si es que se genera por supuesto.

En el caso de los túneles, para su análisis nos basaremos siempre en la documentación de ese segmento que estamos evaluando, sobre la misma debemos identificar su arquitectura y reconocer los dispositivos de entrada y salida de ese túnel, una vez que los identifiquemos, nos conectaremos a ellos y analizaremos sus interfaces, por último si es posible, realizaremos escuchas de tráfico sobre ese segmento de red para verificar si de forma paralela se encuentra algún tipo de tráfico que no esté adecuadamente tunelizado.

Las evidencias que nos van quedando, son los archivos de configuración de los elementos o sus interfaces, los Logs de acceso (vía telnet, ftp, etc), y también las capturas donde se hayan presentado estos hechos, las cuáles deberán ser correctamente filtradas para guardar únicamente las tramas o protocolos que evidencien el hecho, descartando todo lo demás.

El tema de las evidencias, es fundamental para el trabajo de seguridad, pues en general se suele poner en duda o negar este tipo de hechos, pues frecuentemente estamos sacando a flote aspectos que no son agradables para los responsables de estos elementos. Nuestra experiencia nos demuestra que cuanto menos se pueda poner en duda cualquier recomendación que hagamos, más efectiva será la medida correctora, o las acciones que se deriven de esta recomendación, por el contrario, si no somos capaces de demostrar de forma contundente e indiscutible que hay una brecha de seguridad, en este último caso, entraremos en el terreno de la discusión, el debate y por supuesto la evasión de responsabilidades y obligaciones, perdiendo gran parte del efecto deseado.

8. Seguridad en Centrales o Salas de red

8.1. Presentación

En cuanto al desarrollo teórico de este punto, lo tenemos presentado en el Anexo 2 (*Consideraciones a tener en cuenta en un CPD*) del libro "**Seguridad por Niveles**".

Los párrafos que siguen a continuación, son los aspectos sobre los que deberemos centrar la atención y los puntos de control respectivos a considerar en cada sitio donde se alojen dispositivos de red.

La visión de este capítulo, nuevamente debemos mencionar que se trata de una arquitectura distribuida geográficamente de una gran red, pero como ya hemos reiterado, siempre es más positivo poder conocer un despliegue de esta magnitud para luego ajustarlo a una infraestructura menor, que el caso inverso.

Los puntos sobre los que deberíamos centrar nuestra atención son los que presentamos a continuación.

8.2. Ubicaciones

a) Adecuada redundancia de centrales.

Verificar que los servicios que se prestan están debidamente redundados en diferentes ubicaciones físicas. No debemos olvidar que la "disponibilidad" es un parámetro clave de la Seguridad.

b) Adecuada redundancia geográfica.

Verificar que las diferentes ubicaciones físicas se encuentren lo suficientemente distanciadas como para que ante una catástrofe, al menos una de ellas no quede afectada.

c) Adecuada seguridad del entorno.

El concepto de "entorno" no quiere decir seguridad perimetral, sino los alrededores de esa central. Es importante ante cualquier incidencia, que el personal y el material necesario pueda llegar y desplazarse desde y hacia la central a cualquier hora, bajo cualquier inclemencia climática, por caminos accesibles, de forma relativamente segura (*sin jugarse la vida*), etc. Por lo tanto el aspecto a considerar aquí es justamente este tipo de "facilidades" que presenta o no el ámbito que rodea a la central.

8.3. Seguridad en los accesos físicos al edificio.

a) Personal de vigilancia.

Verificar que el personal asignado sea el adecuado (*en cuanto a número y capacidades*), que conozcan su misión, que cumplan lo establecido, que conozcan los procedimientos ante emergencia, sus funciones y responsabilidades.

b) Sistemas de vigilancia.

Verificar la existencia de sistemas de alarmas, de alumbrado, de monitorización, y que los mismos sean adecuados para cada central.

c) Sistemas de comunicaciones (para avisos, alertas, ayuda, evacuación, etc).

Verificar que posean sistemas de comunicaciones, de ser posible redundantes, para emplearlos ante cualquier incidente o anomalía, que se conozca su empleo y se cuente con las cadenas de llamadas correspondientes.

d) Sistemas de autorización de accesos

Se ha podido verificar la existencia de diferentes metodologías para esta actividad con mayor o menor grado de eficiencia. Lo que debe quedar claro aquí es que el control de acceso a una central debe responder "sí o sí" a un proceso riguroso que finalice con la verificación y el registro por parte del personal *(o sistema*) que físicamente abra esta puerta a la central. No se puede admitir que alguna persona que no forme parte del personal de esa central acceda a la misma, sin un flujo de autorización adecuado.

e) Seguridad perimetral.

Verificar el conjunto de medidas de seguridad perimetral (Puertas de acceso, muros, vallado, alumbrado, cámaras, etc.).

f) Controles cruzados para la autorización y verificación del acceso.

Como se ha mencionado en otros capítulos, esta actividad es fundamental y más aún en una central, pues justamente ene stas instalaciones suele necesitar acceder los perfiles más dispares de personas (técnicos,

transportistas, electricistas, mantenimiento, limpieza, fontanería, casi cualquier rol que podamos imaginar. Cuando se suceden este tipo de situaciones, es donde más sencillo es falsificar documentación o pasos para lograr el ingreso. Tengamos en cuenta que una central de comunicaciones es el verdadero "corazón" de toda la red. Para mejorar aún más esta medida, se presenta este aspecto como un nuevo punto de control, con la intención de generar un "flujo cruzado" para esta actividad. Por lo tanto el mensaje a dejar sobre este control, es que independientemente de las medidas que actualmente se estén llevando a cabo para el control de acceso a centrales, en el futuro próximo deberán poder confrontarse o cruzarse con otras, incrementando este nivel de seguridad.

g) Registros de entrada y salida.

Verificar que ese tipo de registros sea el adecuado, permita realizar seguimiento de la actividad, no pueda ser alterado, evadido o borrado. A futuro sería deseable que estos registros se encuentren automatizados, para poder obtener informes, estadísticas, o correlacionarlos con otro tipo de información.

h) Nivel de granularidad de los permisos (controles, áreas, horarios, plazos, actividad a realizar, acompañamientos, etc).

En general hemos podido verificar una gran disparidad en esta medida. Lo que se busca en este control, es que los accesos respondan al flujo que se ha mencionado en puntos anteriores, y que a su vez posea el nivel de granularidad adecuado como para que se acote al máximo posible la actividad de la persona que esté ingresando, intentando que el acceso a la zona o dispositivo final y la actividad que realice no implique un riesgo innecesario.

i) Entrada y salida de material (control y registros).

En este control se debe verificar la existencia de procesos y mecanismos que regulen y dejen sentada por escrito esta actividad, que lo regulado coincida con la realidad, verificando con todo el detalle posible algunos casos concretos de entrada y salida de estos elementos.

j) Plan de actuación ante incidencias.

Verificar la existencia de este plan, el grado de conocimiento que posee el personal que esté a cargo de esa central y también los registros existentes sobre incidencias ocurridas.

k) Cadenas de llamada y escalado de incidencias.

Verificar su existencia, actualización y conocimiento por parte del personal.

8.4. Control medioambiental.

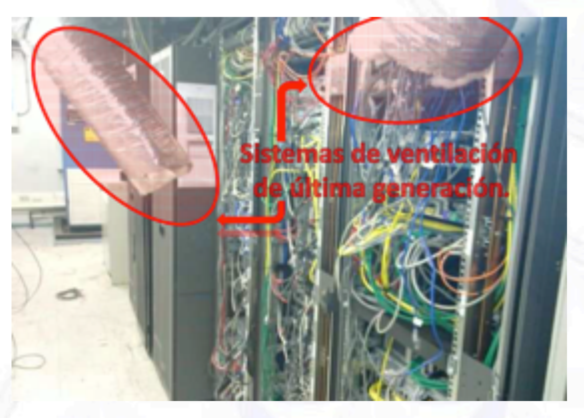




a) Medidas Contra incendio (nivel de detección, automatización, respuesta).

Verificar su eficiencia, funcionamiento, mantenimiento y documentación.

b) Medidas de climatización (Definición y distribución de zonas/pasillos fríos y cálidos, sistemas de emergencia, controles de temperatura).



Verificar su eficiencia, funcionamiento, mantenimiento y documentación. En la actualidad se está minimizando muchísimo el tamaño de los elementos que antes desempeñaban la misma función, en virtud de ello van quedando disponibles grandes sitios en las centrales que suelen ser re aprovechados con otros dispositivos. Esto nos suele llevar a situaciones en las cuáles, el diseño inicial de una sala cambia radicalmente, con los problemas que ello representa. En cuanto al diseño de climatización (y también el de energía), este suele ser uno de los que más sufre estas modificaciones.

c) Medidas de control de humedad.

Verificar su eficiencia, funcionamiento, mantenimiento y documentación. La humedad es el principal enemigo de los elementos electrónicos y también de las fibras ópticas.

d) Medidas adicionales (Lluvias, granizos, temblores, nieve, hielo, etc... en las ubicaciones que sean necesarias).

Verificar su eficiencia, funcionamiento, mantenimiento y documentación.

8.5. Seguridad interna de salas.

a) Medidas de control de acceso a la sala.

Independientemente del acceso físico a la central, es importante que existan mecanismos de control de acceso a cada una de las salas donde están ubicados los servidores, los elementos de red, los grupos electrógenos, los sistemas de ventilación, las salas de control, etc.

b) Presencia y control por parte de personal técnico.

En las salas donde residen sistemas y elementos de red, en general se encuentra presente (*o debería*) personal responsable de su mantenimiento. En este punto lo que se busca es verificar que este personal, conoce sus funciones y responsabilidades y a su vez si participa o no como elemento de control de accesos: Verificando, acompañando, abriendo puertas, salas, racks, etc.

c) Segmentación/separación accesos en áreas o plataformas.



Es importante poseer cierto tipo de lógica en cuanto a la distribución de servicios o funciones de las plataformas o infraestructuras de red. Lo que se presenta aquí, es la verificación de diferentes mecanismos de segregación de los mismos, por medio de salas diferentes, líneas de racks, "jaulas", etc.

d) Seguridad perimetral de sala.

Independientemente de la seguridad perimetral de la central, cada sala debe responder a su vez de medidas de seguridad físicas adecuadas en cada una de ellas.

e) Sistemas de monitorización/videovigilancia interna.

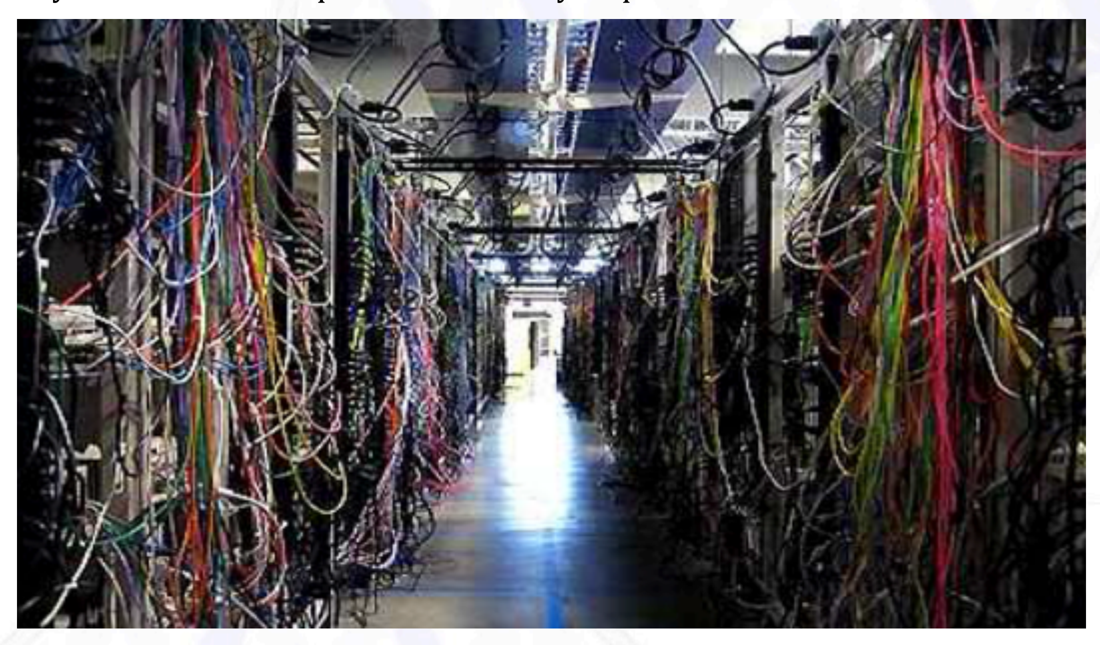
Dentro de las salas es importante poder monitorizar la actividad del personal que se encuentra realizando cualquier actividad, por lo tanto lo que se desea verificar aquí es que se esté en capacidad de hacer este seguimiento.

f) Sistemas de acometida y distribución de red de energía y datos.

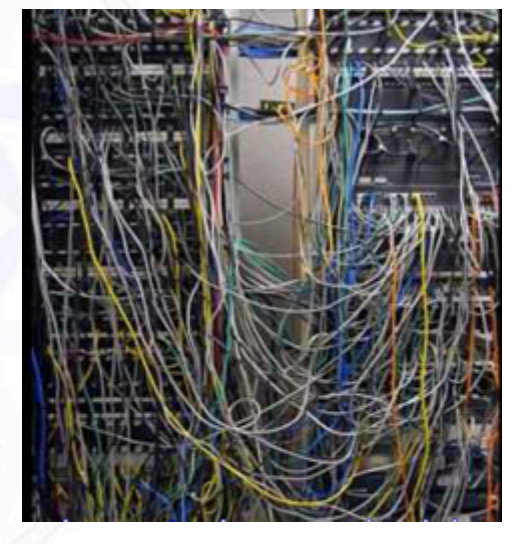
Verificar aquí que la "llegada" de estos cables, fibras, canales, conductos, etc. Se encuentren debidamente segmentados, separados, señalizados, etc.

g) Orden general en el cableado.

Este tema que puede parecer trivial, es de suma importancia, y de hecho ha sido foco de grandes incidencias de seguridad, pues donde hay desorden es muy difícil identificar qué es lo correcto y lo qué no lo es.



La presencia de "latiguillos" puentes, puertos abiertos, cables anónimos, cajas, paquetes, manuales, papeles, hardware anónimo apagado, obsoleto, ordenadores, portátiles, pantallas, teclados, ratones, puntos de acceso, que no están debidamente identificados ocasiona SIEMPRE problemas con buena o mala intención. Un cable tirado por el suelo, seguramente será pisado, cortado, tirado. Un cableado en total desorden dificulta seriamente su manipulación o genera conexiones que nadie sabe para que están. Un sistema de ventilación "provisorio" cuyos cables están por el suelo, que lleva meses tarde o temprano fallará o generará sobrecargas, o mal funcionamiento, etc.



Este punto debería ser controlado con sumo detalle y dejarlo claramente abierto como acción de mejora y seguimiento, para que se pueda aspirar en el

largo plazo a contar con centrales debidamente "ordenadas" e identificados todos sus elementos, sistemas, cables, fibras, puertos, etc.

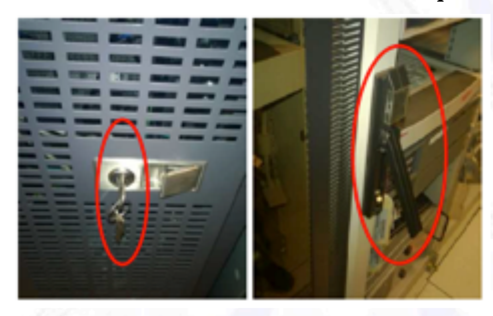
8.6. Seguridad en los Racks de comunicaciones

a) Seguridad física de los racks (llaves, sistemas de cierre).



Los racks de comunicaciones, deberían encontrarse cerrados con llave y contar con algún mecanismo que permita la entrega de las mismas de acuerdo al flujo de acceso de la persona que deba operar dentro de este.

Es importante que este mecanismo minimice fallos, es decir que la llave JAMÁS, deje de encontrarse bajo ninguna circunstancia, pues también este tema es foco de incidencias, cuando se debe operar con premura sobre un elemento del rack y no se encuentra la llave.



b) Ausencia/oscuridad de datos (No direcciones IP, usuarios, contraseñas, redes, configuraciones, etc).

Es un hecho bastante común, encontrar información que en algunos casos puede ser importante, sobre nombres, direcciones, usuarios, etc. Se debería verificar aquí que no se presente ningún tipo de información de este tipo.

c) Metodología/sistemas/plataformas de identificación de cableado (nivel de integración con sistema de inventario y/o creación de planta).

Se reitera este tema nuevamente, pero ahora acotado a cada uno de los racks. Si aún la red no posee con un flujo de identificación del cableado, es motivo de una acción de mejora y seguimiento el contar al mediano plazo con ello.

d) Orden en el cableado y ubicación de dispositivos.

Se desea verificar aquí que dentro del rack de comunicaciones, la ubicación de los dispositivos, sus canaletas, bandejas, su cableado, etc. Se encuentre respondiendo a una lógica adecuada, esté ordenado y precintado.

e) Adecuada distribución/separación de energía y datos.

Todo plan de instalación de elementos de telecomunicaciones considera de forma separada el tema de energía y datos. No respetar adecuadamente estas medidas puede generar serios problemas de ruido, distorsión, sobrecarga, temperatura, etc. Por lo tanto lo que se debe verificar aquí es que se encuentre adecuada la instalación física dentro del rack con lo que Ingeniería y planificación haya establecido para esos elementos.

f) Ventilación individual del rack.

La lógica de instalación de los racks de comunicaciones, tal cual hemos mencionado en puntos anteriores, debería responder al concepto de pasillos fríos y calientes, y dentro de cada rack de comunicaciones la ventilación debe cubrir la totalidad de rack, es decir no debe encontrarse acotada a ciertas zonas del mismo.

Este problema suele suceder en relación al crecimiento de un rack que inicialmente fue diseñado para alojar pocos dispositivos y luego se le incorporan más, dejando de lado el rediseño de la ventilación del rack que debe ser dimensionada nuevamente.

Esta situación, se ha detectado que ocurre frecuentemente debido a los continuos cambios de infraestructura de red, por lo tanto se debería prestar especial atención a este detalle.

8.7. Control de energía.

a) Plan de distribución eléctrica.

Redacción, aprobación y existencia del plan.

b) Responsables, obligaciones y funciones.

Verificar su adecuado dimensionamiento y el conocimiento de cada uno de ellos de sus responsabilidades, obligaciones y funciones.

c) Análisis de consumos críticos y evaluación de necesidades críticas.

Verificar que se realice con la frecuencia necesaria un análisis y seguimiento de estos consumos y necesidades para que la respuesta del abastecimiento eléctrico ante cualquier anomalía (*o en estado normal de funcionamiento*) sea la adecuada.

d) Sistemas redundantes de energía.

Verificar que estén debidamente dimensionados, mantenidos, actualizados y monitorizados.






e) Análisis, implantación y segmentación de plataformas/zonas/dispositivos críticos o prioritarios.

Verificar si el sistema de alimentación, se encuentra debidamente "priorizado" hacia el mantenimiento de elementos críticos de red. Este tema ha sido puesto de manifiesto como un problema en algunas redes que hemos conocido en las que los sistemas redundantes de energía ante caídas de la red general, se inician abasteciendo a la totalidad de las salas, con lo cual la durabilidad (*y el coste*) de los mismos no es el óptimo.

Lo que se debe verificar aquí, es que los sistemas redundantes de energía, en el caso de entrar en servicio lo hagan respondiendo a un análisis de la estrategia de negocio, y su abastecimiento responda a un plan debidamente estudiado, y no a un servicio "a granel" sobre la totalidad de los dispositivos de la sala o central. Se recalca este tema pues en general, se trata de sistemas de alto coste que justamente si no se diseñan con máximo detalle, se incurre en errores que causan alto impacto para la organización.

f) Plan de pruebas (y cumplimiento del mismo).

Verificar la existencia del plan, su cumplimiento, los registros y constancias de su implementación.

g) Sistemas de monitorización de energía.

Verificar que existan, sean adecuados, y se estén monitorizando adecuadamente los mismos.

h) Metodología de mantenimiento de los sistemas de energía (planificación, diseño y aplicación).

Sobre este tema se han detectado varios aspectos a tener en cuenta que se relacionan al mantenimiento, aunque parezcan menores, ocasionan graves inconvenientes pues en momentos clave generan fallos. Ejemplos de ello, son reposición de combustible, arranques manuales de generadores, personal capacitado para hacerlo y lugares desde donde puede operar (formas de desplazarse), llaves y metodologías de acceso físico, tiempos hasta que se encienden estos sistemas, etc.

9. Trabajo con diferentes comandos y herramientas.

9.1. Presentación.

En este capítulo presentaremos una serie de herramientas, desarrollos, comandos y ejemplos que hemos considerado pueden ser de utilidad en el trabajo de seguridad en redes. Por supuesto que existen muchísimas más aún, y cada lector también preferirá emplear de otro fabricante, modelo u opciones diferentes de trabajo.

En los párrafos siguientes, sólo es nuestra intención, transmitir algo de lo que en nuestra experiencia nos ha sido de utilidad, pero no es objetivo de este libro, dar un curso detallado del uso de cada una de ellas.

9.2. Kali.

Kali, es una distribución de Linux basada en Debian que reúne un conjunto importante de herramientas de seguridad. Su predecesor fue **Back Track** (*que lamentablemente para los que nos gusta Debian, cambió su base puede fue Slax, basado en Slackware*), Es llamativo este cambio de Back Track hacia Slax, pues este a su vez se basó en gran medida en **Knoppix** que en su momento fue Debian también.

Para el trabajo de Seguridad en Redes, es fundamental tener conocimientos de sistemas operativos basados en distribuciones Linux, pues sin lugar a dudas es con estas plataformas con las que podremos hacer uso de la totalidad de herramientas del mercado libre para cualquier actividad de evaluación, testeo, escaneo, captura de tráfico, programación en lenguajes sencillos y prácticos, etc. En esto (y mucho más) Linux es incomparable.

Recomendamos que el lector instale la última versión de "**Kail**", pues encontrará en él todas las herramientas necesarias para el trabajo de Seguridad en Redes, y nos basaremos en este para todos los ejercicios que siguen. Tengamos en cuenta que así como un intruso las emplea con malas intenciones, las mismas a su vez, como en cualquier otro terreno de operaciones militares, deben ser conocidas en detalle para saber defendernos con las armas y metodologías que emplean para atacarnos.

Las características que lo destacan según su propia Web en Español: http://es.docs.kali.org/introduction-es/que-es-kali-linux son:

- Posee más de 300 herramientas para "Test de Penetración"
- Gratis y siempre lo será
- Git (Sistema Open Source de control de versionado) - árbol de código abierto

- Obediente a FHS (File Hierachy Standard).
- Amplio apoyo a dispositivos inalámbricos.
- Kernel personalizado con parches de inyección.
- Entorno de desarrollo seguro.
- Paquetes firmado con PGP y repositorios.
- Multi-lenguaje.
- Totalmente personalizable.
- Soporte ARMEL y ARMHF (Familias de instrucciones de código reducido).

Puede descargarse desde la siguiente URL: https://www.kali.org/downloads/

Una vez instalado su pantalla inicial se ve de la siguiente forma:

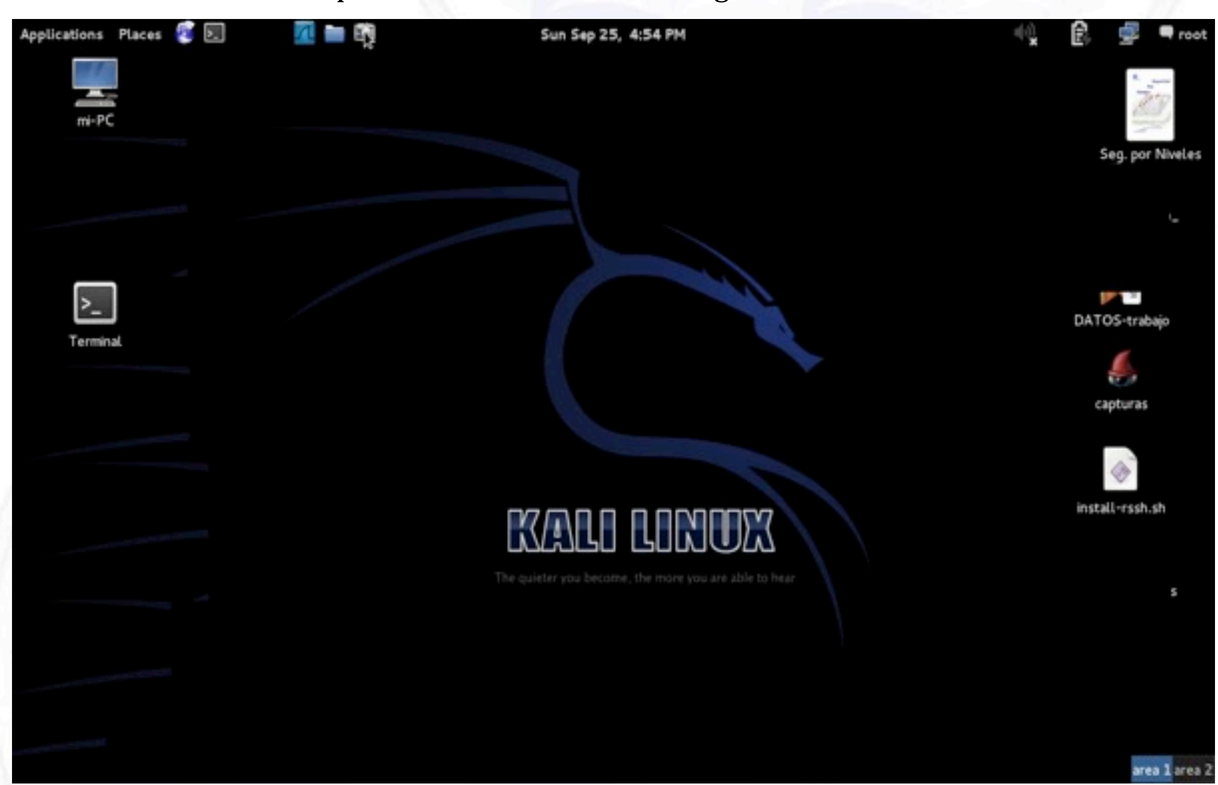


Imagen 9.1 (Portada inicial de Kali)

Si desplegamos sus Aplicaciones, podemos ver el menú "Kali" donde nos ofrece el listado de la clasificación de todas ellas:

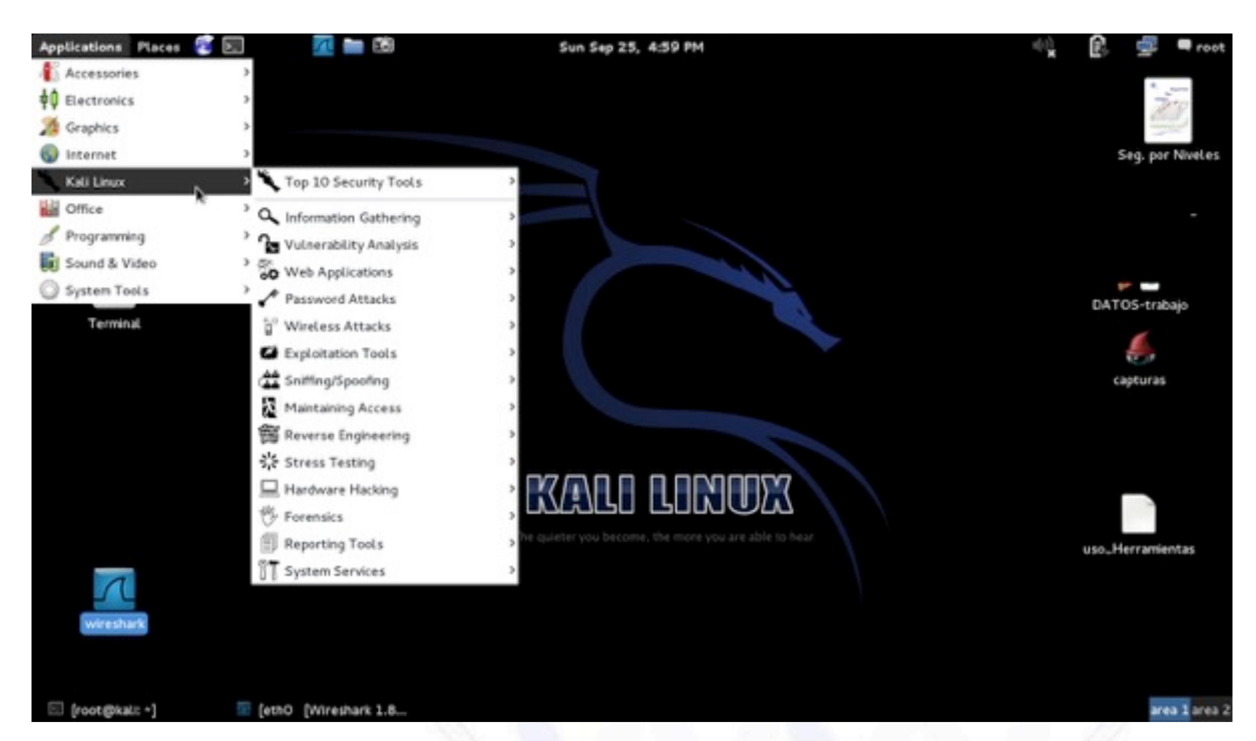


Imagen 9.2 (Despliegue de herramientas de Kali)

Nuestro consejo, antes de decidir si el lector desea o no trabajar de forma permanente con este sistema operativo es que realice una instalación por medio de máquinas virtuales.

En el mercado las dos más conocidas son:

a) Virtual Box.

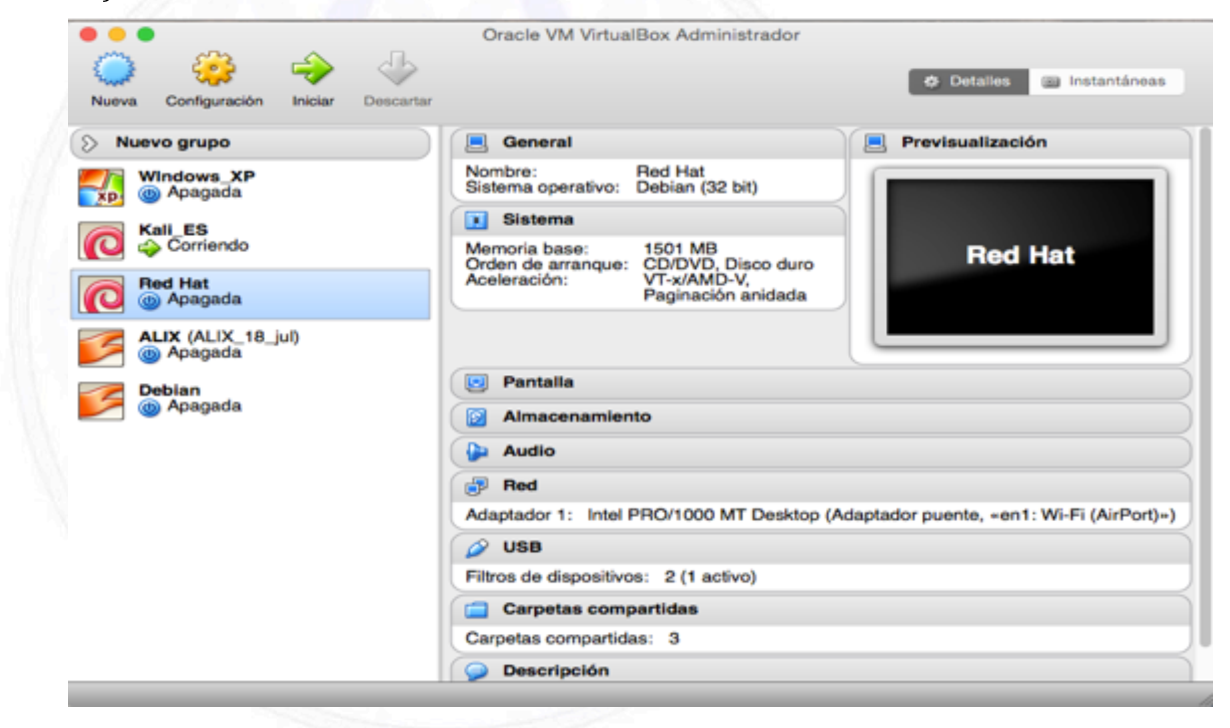


Imagen9.3 (Virtual Box)

b) VMWare

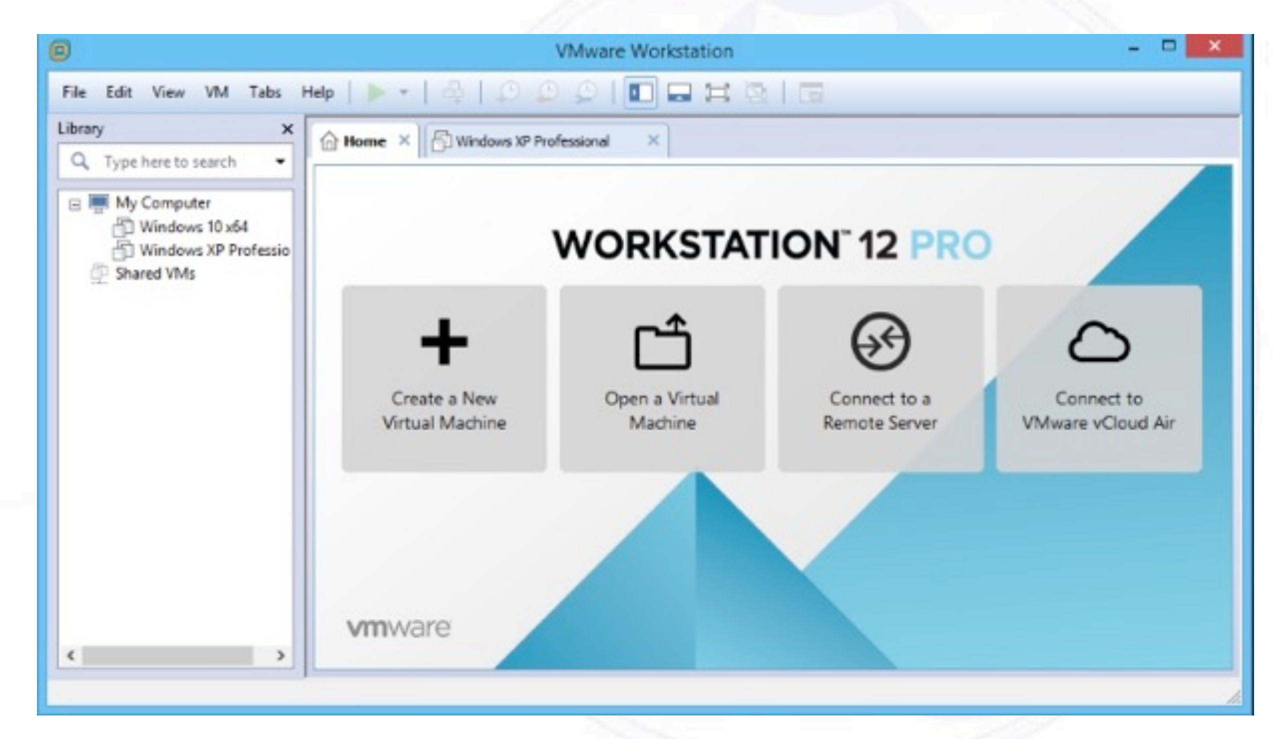


Imagen 9.4 (VMWare)

9.3. Túneles.

La función típica del protocolo de red Secure Shell (**SSH**) es acceder en modo terminal a un sistema remoto y ejecutar allí comandos de forma segura gracias a que los datos van cifrados. Pero además, a través de esa conexión de datos segura, es posible crear túneles (*reenviar puertos / port forwarding*) entre los extremos conectados de forma que las conexiones TCP/IP se encaminan a través de la conexión SSH con esto, se puede conseguir que a través del puerto 22 se "entube" cualquier otro puerto. Esta funcionalidad a su vez permite pasar aplicaciones o puertos que no estén permitidos a través de cualquier firewall o dispositivo de bloqueo de puertos siempre que se tenga la posibilidad de conectar con SSH. El concepto correcto es "redirección de puertos".

Esta tarea también se puede hacer a través de aplicaciones con interfaz gráfica como **PuTTY** o **SecureCRT** que también permiten el reenvío de puertos.

Vamos a presentar en esta sección, una serie de trabajos prácticos que hemos realizado en un seminario sobre este tema, en el cual se montó un sencillo laboratorio para trabajar de forma eminentemente práctica. Para que podamos transmitir lo más claro posible cada una de estas prácticas es que pegamos a continuación el texto de apoyo empleado en este cursillo.

Durante este desarrollo nos centraremos en y por línea de comandos pues es la forma más didáctica de comprender esta actividad, una vez comprendida, es mucho más sencillo emplear la herramienta gráfica que se desee.

Para nuestra práctica vamos a configurar un escenario de la siguiente manera:

a. Punto de acceso WiFi.
b. Sonda Raspberry (que emplearemos como máquina de salto) (10.0.0.101/8) y (192.168.1.34/24).
c. Máquina destino: Kali (en virtual, ejecutándose en mi portátil) (10.0.0.100/8).
d. Participantes (cada uno de los participantes del curso) (192.168.1.1xx/24)

Todos los participantes trabajarán dentro del segmento de red 192.168.1.x/24 (Ej: alumno1: 192.168.1.101/24, alumno 2:192.168.1.102/24, etc.)

La sonda (Raspberry) tiene dos interfaces configuradas: IP1: 192.168.1.34/24, IP2: 10.0.0.101/8

El esquema de este laboratorio es el siguiente:

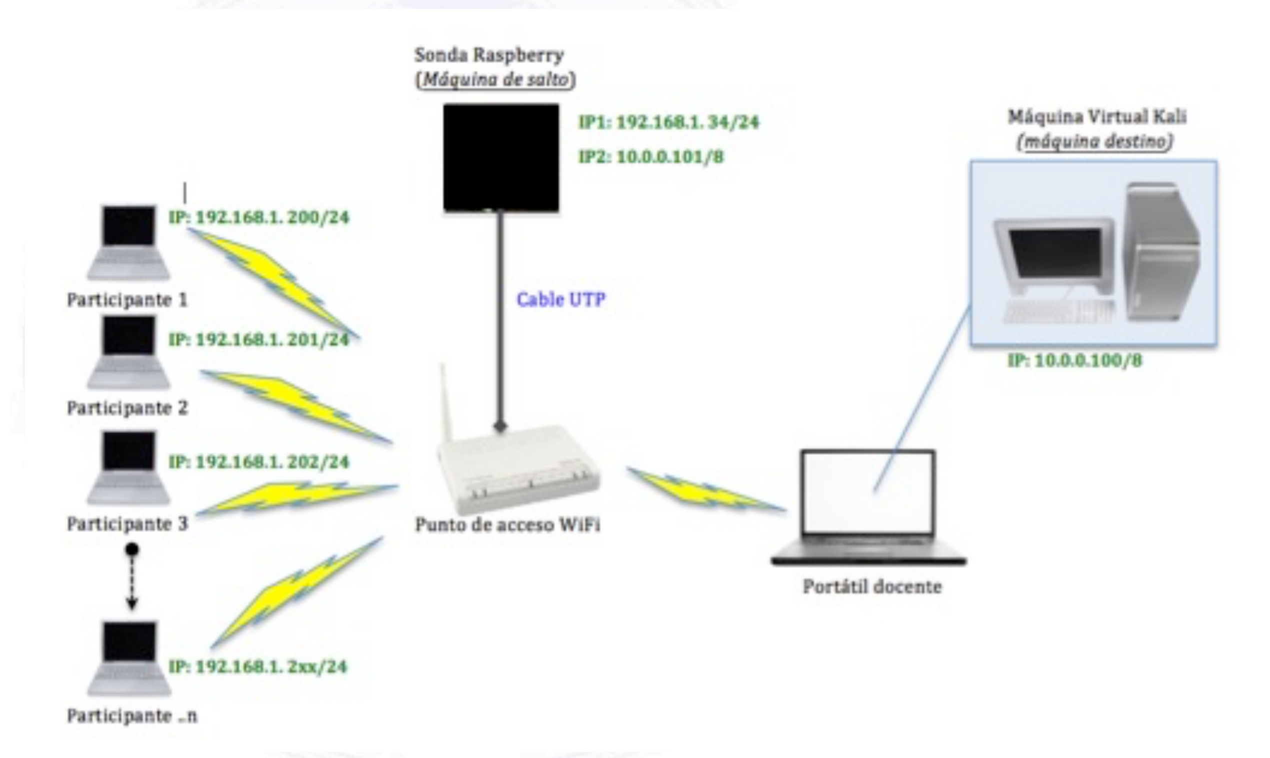


imagen 9.5 (Configuración del Laboratorio para el trabajo de redirección de puertos)

Desde la sonda:

```
#ifconfig -a
     usmsc0 flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
     address: b8:27:eb:9c:31:14
        inet 192.168.34.4 netmask 0xffffff00 broadcast 192.168.34.255
        inet alias 192.168.1.34 netmask 0xffffff00 broadcast 192.168.1.255
        inet alias 10.0.0.101 netmask 0xff000000 broadcast 10.255.255.255
```

Máquina destino *(**Kali** en Máquina virtual instalada en el ordenador del docente*) tiene configurada una única IP configurada: 10.0.0.100/8

Desde esta máquina virtual Kali:

```
root@kali:/etc/apache2# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:ae:3f:c6
          inet addr:10.0.0.100  Bcast:10.255.255.255  Mask:255.0.0.0
```

Por lo tanto, para poder alcanzar la máquina destino por parte de cualquier participante, es necesario que se validen en la máquina de salto (*concepto que hemos desarrollado en el capítulo 7),* pues se encuentran en diferentes segmentos de red la máquina participantes (**192.168.1.2xx/24**) y la máquina destino (**10.0.0.100/8**).

Una vez validado "**dentro**" de la máquina de salto (Raspberry) entonces dependiendo de la red que se desee alcanzar, esta máquina decidirá por que interfaz de red encaminará esos paquetes IP.

Esta máquina virtual Kali tiene configurado un servidor Web apache (*cuyo index.ini está en **/var/www/**)* para que probemos su acceso gráfico a través de la máquina de salto.

Si analizamos las rutas que tiene configurada la máquina de salto veremos lo siguiente:

```
Destination        Gateway            Flags    Refs       Use     Mtu Interface
10/8               link#1             UC          -         -       -L usmsc0
10.0.0.100         68:a8:6d:47:77:1e  UHLc        -         -       -L usmsc0
127/8              127.0.0.1          UGRS        -         -   33192L lo0
127.0.0.1          127.0.0.1          UH          -         -   33192L lo0
192.168.1/24       link#1             UC          -         -       -L usmsc0
192.168.1.1        00:1d:20:0e:5d:df  UHLc        -         -       -L usmsc0
192.168.1.34       68:a8:6d:47:77:1e  UHLc        -         -       -L usmsc0
192.168.34/24      link#1             UC          -         -       -L usmsc0
```

vamos a analizar qué puertos existen abiertos:

a. Máquina de salto:

```
raspberry$ nmap localhost
PORT   STATE SERVICE
22/tcp open  ssh
```

b. Kali (Máquina destino):

```
root@kali:/var/www# nmap localhost
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

c. Máquina participante (en esta caso la portátil del docente):

```
sh-3.2# nmap localhost
PORT      STATE SERVICE
631/tcp   open  ipp
7778/tcp  open  interwise
```

Túneles SSH: comencemos a ver el tema de los túneles

Ejemplo 1:

Comenzaremos con 3 máquinas: A (portátil del docente), B (Salto), C (destino)

Vamos a ver de forma práctica 3 tipos de túneles:

a. Túnel Local
b. Túnel remoto
c. Túnel dinámico

1. Túnel local:

Verifiquemos primero una conexión clásica por ssh.

```
sh-3.2# ssh curso1@192.168.1.34

  raspberry$ whoami
       curso1

  raspberry$ pwd
       /home/curso1
```

```
raspberry$ nmap localhost
PORT   STATE SERVICE
22/tcp open  ssh
```

Prueba 1:

```
ssh -L 1111:127.0.0.1:1111 curso1@192.168.1.34
```

(con esto queda en listen el puerto 1111 en mí máquina)

Si analizo ahora la portátil del docente (Máquina origen):

```
sh-3.2# nmap localhost
PORT      STATE SERVICE
631/tcp   open  ipp
1111/tcp  open lmsocialserver <-se ha abierto un nuevo puerto
7778/tcp  open  interwise
49152/tcp open  unknown
49153/tcp open  unknown
```

Sin embargo si el mismo nmap lo lanzo desde la máquina de salto ¿Qué debería ver???????

```
raspberry$  nmap -p 1111 192.168.1.34
PORT     STATE  SERVICE
1111/tcp closed lmsocialserver
```

¿A qué se debe?

Veamos qué es esto de los puertos Locales......

Analicemos nuestra tabla de puertos:

Para la portátil del docente:

```
sh-3.2# netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  *.*                    *.*                    CLOSED
tcp4       0      0  127.0.0.1.1111        *.*                    LISTEN
tcp4       0      0  192.168.1.40.60893    192.168.1.34.22       ESTABLISHED
tcp4       0      0  127.0.0.1.7778         *.*                    LISTEN
tcp4       0      0  127.0.0.1.29754        *.*                    LISTEN
tcp4       0      0  127.0.0.1.49153        127.0.0.1.1023         ESTABLISHED
tcp4       0      0  127.0.0.1.1023         127.0.0.1.49153        ESTABLISHED
tcp4       0      0  127.0.0.1.49153        *.*                    LISTEN
tcp4       0      0  127.0.0.1.49152        *.*                    LISTEN
tcp4       0      0  127.0.0.1.631          *.*                    LISTEN
```

Para la máquina de salto:

```
raspberry$ netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        State
tcp        0      0  192.168.1.34.22      192.168.1.40.60893   ESTABLISHED
tcp        0      0  *.22                   *.*                    LISTEN
udp        0      0  *.*                    *.*
```

Si analizo la máquina de salto:

```
raspberry$ nmap localhost
PORT   STATE SERVICE
22/tcp open  ssh
```

Vemos que sigue igual…..

Volvamos a analizar el comando y representémoslo en una imagen.

```
ssh -L 1111:127.0.0.1:1111 curso1@192.168.1.34
```

(con esto queda en listen el puerto 1111 en la máquina del docente)

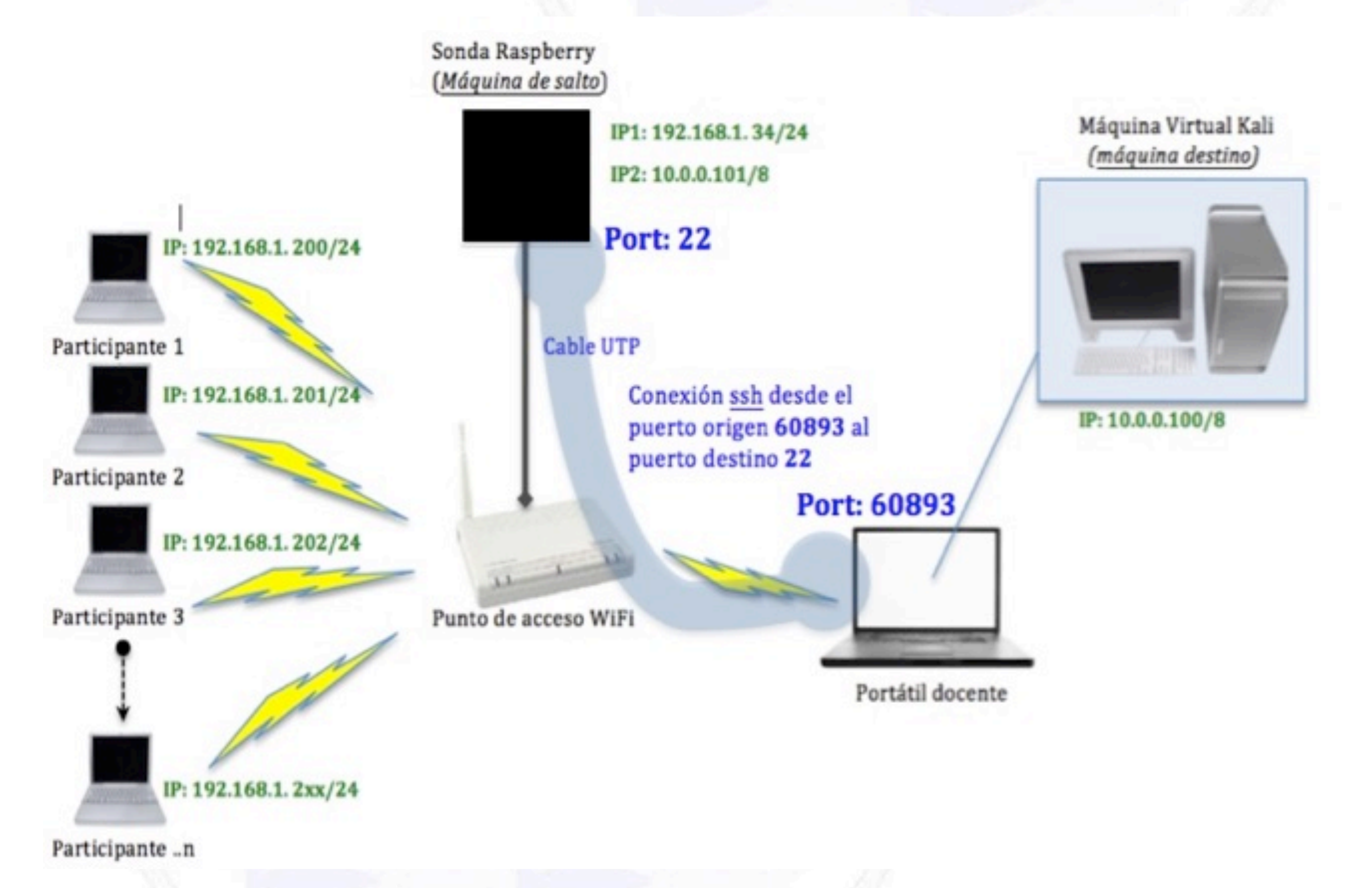


Imagen 9.6 (Túnel SSH)

El comando que acabamos de ejecutar, vamos a pensarlo como compuesto por dos partes:

```
ssh -L 1111:127.0.0.1:1111 curso1@192.168.1.34
```

parte 1: `ssh -L 1111:127.0.0.1:1111 curso1@192.168.1.34` (en color negro)

Es cuando se establece la verdadera sesión tcp (con su triple handshake) desde el puerto origen, en nuestro caso 60893 y puerto destino 22. Esta es la única sesión que se establece entre ambos dispositivos, tal cual nos lo presentó la tabla de sesiones:

tcp 0 0 192.168.1.34.22 192.168.1.40.60893 ESTABLISHED (en Máq salto)

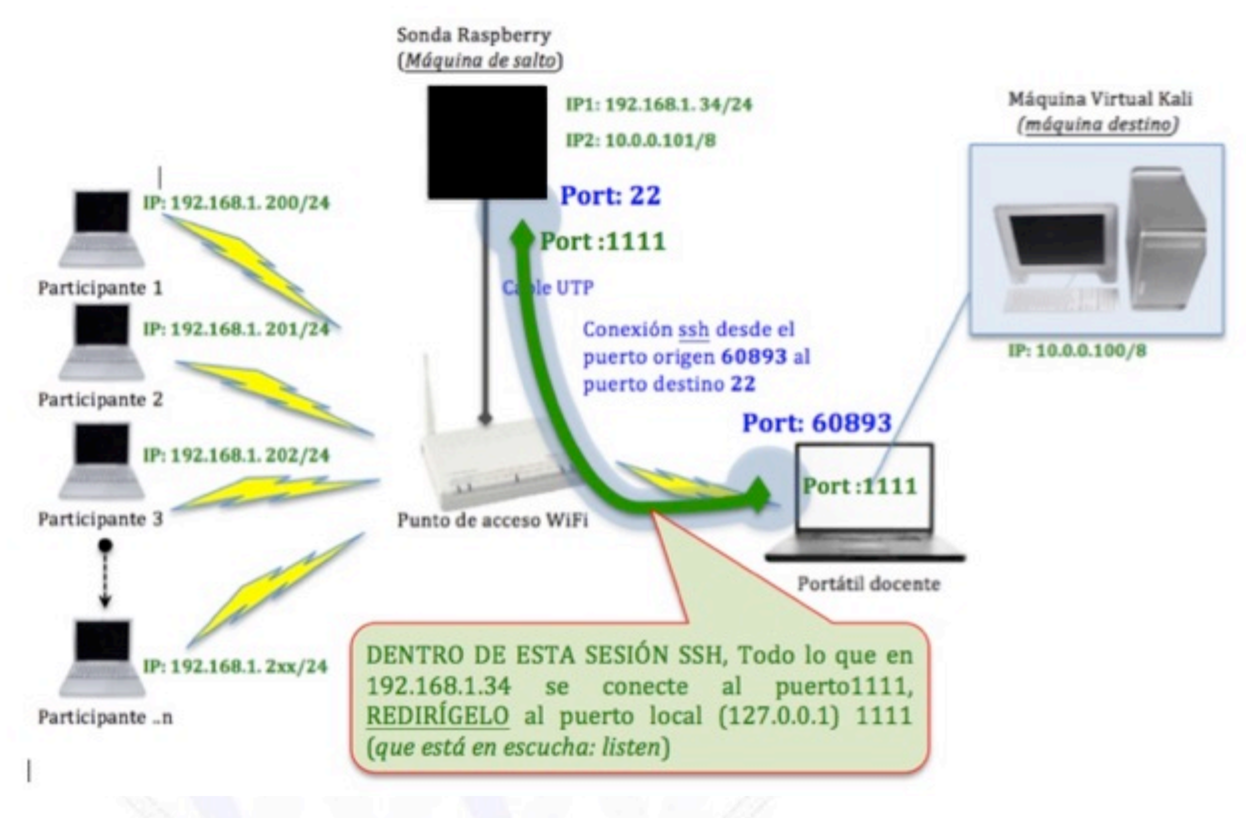
tcp4 0 0 192.168.1.40.60893 192.168.1.34.22 ESTABLISHED (en portátil del docente)

Luego (la otra parte):

`ssh -L 1111:127.0.0.1:1111 curso1@192.168.1.34`

parte 2: `ssh -L 1111:127.0.0.1:1111 curso1@192.168.1.34` (en naranja)

Es cuando le indicamos que <u>deje en escucha</u> para <u>mi localhost</u> (127.0.0.1) el puerto 1111, y redirija todo la información que la máquina destino encamine hacia el 1111 de esta última, tal cual se presenta en la imagen que sigue a continuación:



<u>Imagen 9.7 (Redirección dentro del túnel SSH)</u>

Veamos una aplicación más concreta de esta situación:

Ejemplo 2:

Necesito ejecutar una aplicación en la red destino que se ofrece, por ejemplo, a través del puerto 80, pero la máquina de salto sólo habilita la conexión por el puerto 22 (caso muy real y concreto).

En nuestro laboratorio, la máquina virtual "Kali" (IP: 10.0.0.100/8) tiene configurado un servidor apache en el puerto 80. Una portátil de participante no tiene visibilidad con ella pues su IP será del rango:192.168.1.2xx, por lo tanto para poder abrir esta Web deberá conectarse primero a la máquina de salto a través de su interfaz 192.168.1.34 y desde este dispositivo intermedio sí es visible la IP y el puerto 80 de "kali".

Primero verifiquemos estos conceptos:

```
Participante# ping 10.0.0.100
     PING 10.0.0.100 (10.0.0.100): 56 data bytes
     92 bytes from 192.168.1.1: Destination Net Unreachable

Máq de salto$ ping 10.0.0.100
     PING 10.0.0.100 (10.0.0.100): 56 data bytes
     64 bytes from 10.0.0.100: icmp_seq=0 ttl=64 time=4.281000 ms
     64 bytes from 10.0.0.100: icmp_seq=1 ttl=64 time=61.297000 ms

Kali# ping 10.0.0.101
     PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data.
     64 bytes from 10.0.0.101: icmp_req=1 ttl=255 time=5.09 ms
     64 bytes from 10.0.0.101: icmp_req=2 ttl=255 time=10.1 ms
```

Tenemos dos opciones. Para continuar con el empleo de puertos locales, veremos la primera de ellas nuevamente a través de la opción **"-L":**

- Opción 1:

desde PC *Participante# ssh -L 8000:10.0.0.100:80 curso1@192.168.1.34*

Abro Firefox **sin proxy** en localhost (http://localhost):

localhost:8000

Esta es una página Web creada para prueba del curso de red 2016

Esta es la página por defecto.

Este servidor Web no contiene más información.

Imagen 9.8 (Acceso a interfaz Web por medio de un túnel SSH)

¿Qué hemos hecho?

Analicemos nuevamente el comando parte por parte:

`ssh -L 8000:10.0.0.100:80 curso1@192.168.1.34` (en color azul):

Hemos establecido una sesión ssh entre un puerto origen cliente (*supongamos el puerto el puerto 33120*) y el puerto destino 22 desde la máquina del Participante 1 hasta la sonda Raspberry (Máquina de salto).

`ssh -L 8000:10.0.0.100:80 curso1@192.168.1.34` (en color azul):

Deja en escucha en mi ordenador (Participante 1, *desde donde se lanzó el comando*) el puerto 8000 y redirige al mismo todo lo que venga de la dirección IP 10.0.0.100 desde el puerto destino 80.

Luego abrimos Firefox para que nos presente la información que tenga en localhost en el puerto 8000. Tened en cuenta que por defecto el protocolo http establece sesiones hacia el puerto 80, pero la información que tenemos es la que se está REDIRIGIENDO del puerto destino 80 en la ip 10.0.0.100 hacia el puerto 8000 por lo tanto debemos aclarar **http://localhost:8000**, tal cual se representa en la imagen que sigue:

DENTRO DE ESTA SESIÓN SSH, Todo lo que se reciba desde la IP 10.0.0.100 desde el puerto destino 80, REDIRÍGELO al puerto local "-L" 8000 de la máquina desde la que se lanzó el comando (*que está en escucha: listen*)
Sonda Raspberry
(*Máquina de salto*)
IP1: 192.168.1.34/24
IP2: 10.0.0.101/8
Máquina Virtual Kali
(*máquina destino*)
Port : 8000
Port: 33120
Port: 22
IP: 192.168.1.200/24
Port : 80
Participante 1
Cable UTP
IP: 192.168.1.201/24
IP: 10.0.0.100/8
Participante 2
IP: 192.168.1.202/24
Participante 3
Punto de acceso WiFi
Portátil docente
IP: 192.168.1.2xx/24
Participante ..n

Imagen 9.9 (Redirección del túnel SSH)

- Opción 2:

En esta opción emplearemos el concepto de redirección "**Dinámica**" de puertos, que como su nombre lo indica nos facilitará mayor dinamismo o flexibilidad para esta redirección. Es decir, no solamente estará asociada a un puerto y dirección destino específica, sino que nos permitirá "redirigir" cualquier destino hacia el puerto local que le indiquemos.

Veámoslo con un ejemplo:

Deseo alcanzar el mismo servidor Web que en el caso anterior, pero para la redirección dinámica ahora empleаré la opción "**-D**" y con el formato que se presenta a continuación:

```
ssh -D 127.0.0.1:1080 curso1@192.168.1.34
```

Abro Firefox sin proxy, pero con proxysocks en 127.0.0.1: 1080 (http://IP_destino)

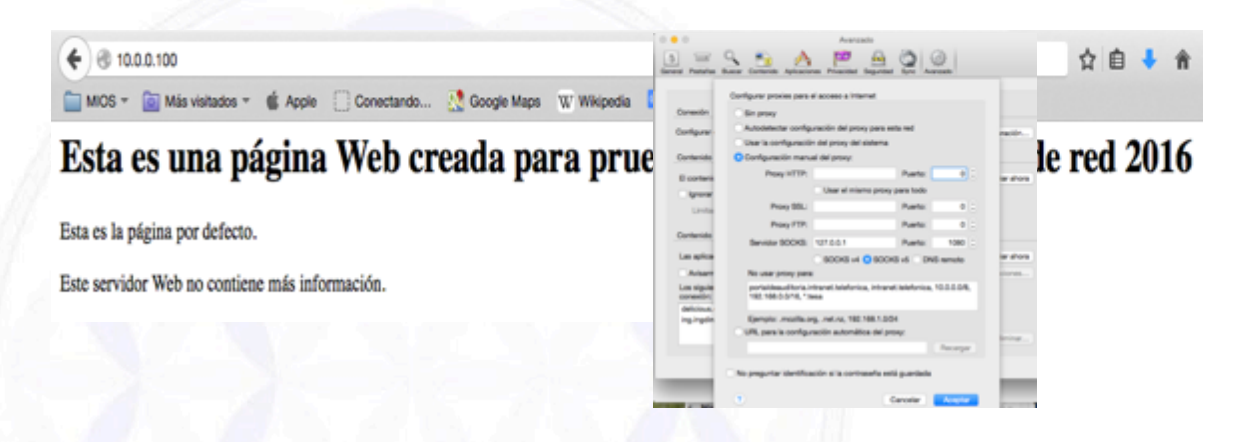


Imagen 9.10 (empleo de proxysocks)

¿Qué sucedería si deseara acceder a otro servidor Web de esa red destino?........

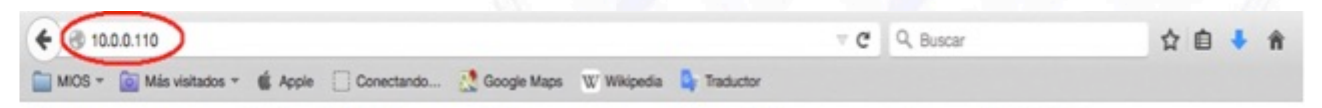
Por tratarse de un redireccionamiento dinámico de puertos, podré hacerlo sin problema, pues tal cual nos muestra la línea de comandos que ejecutamos (ssh -D 127.0.0.1:1080 curso1@192.168.1.34) ahora no estamos aclarando ningún tipo de puerto ni dirección destino, por lo tanto la máquina 192.168.1.34 (máquina de salto) encaminará toda la información que reciba hacia el puerto 1080 del otro extremo de la sesión tcp.

Para verificar este hecho, vamos a conectarnos a otro servidor Web en otra dirección IP.

(Para este ejemplo, en nuestro Laboratorio, cambiaremos la dirección IP de "Kali"):

```
root@kali:/etc/apache2# ifconfig eth0 10.0.0.110 netmask 255.0.0.0
root@kali:/etc/apache2# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:ae:3f:c6
          inet addr:10.0.0.110  Bcast:10.255.255.255  Mask:255.0.0.0
```

Ahora sin tocar nada en el navegador del PC del participante, nos podemos conectar a esta nueva dirección IP:



Esta es una página Web creada para prueba del curso de red 2016

Esta es la página por defecto.

Este servidor Web no contiene más información.

Imagen 9.11 (empleo de túnel SSH Dinámico)

Podemos analizar toda esta secuencia con una captura de tráfico realizada desde la máquina "Participante" (*ver: tunel_dinamico-port80_filtrado.pcap que podemos descargar desde la Web:* http://www.darFe.es).

Ejemplo 3:

Para realizar este ejercicio, damos por sentado que el lector tiene instalado una máquina con sistema operativo "Kali", le configuramos una cuenta "curso" con contraseña "curso". En este curso si empleamos estas máquinas, por lo tanto podemos suponer que en el laboratorio que tenemos montado la "máquina destino" es posible que también tenga esta misma cuenta *(¿se habrá enterado el docente……? Pues está en su mismo ordenador….).*

Nuestro objetivo será emplear la máquina de salto para conectarnos vía ssh a la máquina destino………. Pero sin ejecutar los comandos en la máquina de salto, sino en la local. Veamos el caso:

Desde la máquina Participante ejecutamos:

Participante# ssh -L 2222:10.0.0.100:22 curso1@192.168.1.34

Y desde la misma máquina:

Participante# ssh -p 2222 curso@localhost

```
pruebas — curso@kali: ~ — ⌘1
curso@kali: ~
sh-3.2# ssh -p 2222 curso@localhost
curso@localhost's password:
Linux kali 3.7-trunk-686-pae #1 SMP Debian 3.7.2-0+kali5 i686

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan 26 15:53:01 2016 from 10.0.0.101
curso@kali:~$ version
-bash: version: no se encontró la orden
curso@kali:~$ uname -a
Linux kali 3.7-trunk-686-pae #1 SMP Debian 3.7.2-0+kali5 i686 GNU/Linux
```

Imagen 9.12 (interfaz de comandos)

Ejemplo 4 (Empleo de túnel Remoto "**-R**"):

Supongamos que existe un dispositivo que no nos permite realizar conexiones desde el exterior hacia el interior. En nuestro caso por ejemplo "Kali" puede estar dentro de una Intranet sobre la que está filtrado el establecimiento de sesiones desde el exterior.

En nuestro laboratorio, si tenemos acceso a esta máquina exterior (Máquina de salto) desde dentro de la Intranet (Kali), podríamos abrir en esta caso una "redirección Remota" y ahora sí dejamos en escucha un puerto con una conexión que se ha establecido desde dentro hacia fuera. Veamos el ejemplo:

desde Kali# ssh -R 8080:localhost:22 curso1@10.0.0.101

desde Participante#ssh -L 9090:localhost:8080 curso2@192.168.1.34

```
raspberry$ whoami     ←  sonda (Máquina salto)
        curso2
raspberry$ netstat -an
```

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address      Foreign Address        State
tcp    0      0  192.168.1.34.22      192.168.1.40.53714     ESTABLISHED
tcp    0      0  127.0.0.1.8080       *.*                    LISTEN
tcp    0      0  10.0.0.101.22         10.0.0.100.60983       ESTABLISHE
tcp    0      0  *.22                  *.*                    LISTEN
```

Si analizamos la tabla de rutas de la portátil del Participante veremos:

```
sh-3.2# netstat -an |grep 9090
     tcp4   0      0  127.0.0.1.9090          *.*                 LISTEN
     tcp6   0      0  ::1.9090                *.*                 LISTEN
```

Nuevamente desde *Participante#ssh -p 9090 curso@localhost* (passwd curso)

```
curso@localhost's password:
     Linux kali 3.7-trunk-686-pae #1 SMP Debian 3.7.2-0+kali5 i686

     The programs included with the Kali GNU/Linux system are free software;
     the exact distribution terms for each program are described in the
     individual files in /usr/share/doc/*/copyright.


     Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
     permitted by applicable law.
     Last login: Tue Jan 26 17:19:37 2016 from localhost
curso@kali:~$
curso@kali:~$ whoami
             curso

curso@kali:~$ netstat -an
     Active Internet connections (servers and established)
     Proto Recv-Q Send-Q Local Address          Foreign Address        State
     tcp     0      0 0.0.0.0:22             0.0.0.0:*              LISTEN
     tcp     0    628 10.0.0.100:60983     10.0.0.101:22          ESTABLISHED
```

<u>Parte 2.</u> <u>Escaneos a través de máquinas de salto (empleo de tsoks)</u>

Comando "**tsoks**"

Continuando con el mismo esquema de laboratorio, para usar la Raspberry como más salto (*operando desde la Kali de los alumnos*), debemos configurar el archivo **<u>"tsocks.conf":</u>** (en Kali está en **/etc**).

```
local = 127.0.0.0/255.0.0.0
local = 192.168.1.0/255.255.255.0
server = 127.0.0.1
server_type = 5
server_port = 8080
```

Abrimos el puerto 8080 en nuestro localhost y nos conectamos al puerto 22 de la IP 192.168.1.34 (Raspberry salto) realizando la siguiente secuencia de acciones:

1) `ssh -C -D 127.0.0.1:8080 pi@192.168.1.34 -p 22`

2) lanzamos "**tsocks on**"

3) `tsocks nmap -PN -n -sT -p 80 10.0.0.100` (IP destino de nmap)

4) al finalizar la actividad ejecutamos "`tsocks off`"

9.4. Cómo evaluar SNMP.

Ya hemos visto que con los ficheros de configuración en nuestro poder, a través de los script en bash que presentamos en el capítulo de "routing" podemos evaluar el nivel de seguridad en las configuraciones de nuestra red.

Otra forma de analizar este protocolo, es en remoto, en particular por ejemplo cuando evaluamos comunidades y mensajes del protocolo snmp, para este trabajo lo debemos hacer a través del análisis del puerto **UDP 161** (*aunque también emplea el puerto UDP 162, pero este es para el envío de Traps snmp*). Por lo tanto lo primero que tenemos que verificar es qué dispositivos tienen abierto este puerto, para ello emplearemos el comando "**nmap**" de la siguiente forma:

```
# nmap –sU  -p 161 IP/Red_destino –sV
```

La opción "**-sU**" es para que el escaneo lo realice mediante UDP , la opción "**-p 161**" es para que sólo busque este puerto, y por último (*muy importante*) la opción "**-sV**" nos dirá la versión de snmp y, si la comunidad es por defecto (public o private), nos informará también.

A continuación, empleando el comando "**snmpwalk**" (que por defecto está instalado en Kali), nos permitirá acceder a toda la información de snmp, que esté ofreciendo la MIB de ese destino. Indicando con el parámetro "-v" la versión (1,2c o 3) y con el parámetro "-c" la comunidad (public o cualquiera que conozcamos previamente).

```
snmpwalk -c public -v 1 IP_destino system
```

9.5. Wireshark.

Este software, imprescindible para todo trabajo de red, ya lo hemos presentado con bastante nivel de detalle, y realizado una serie de prácticas en el libro "**Seguridad por Niveles**", también hemos visto su empleo en el capítulo 1 en lo referente a VoIP (*esta de hecho es una nueva funcionalidad que en año 2011 cuando presentamos el libro anterior, aún*



no estaba incorporada a esta herramienta) por lo tanto en esta sección sólo presentaremos aspectos recientes de la misma, con la intención de ofrecer opciones que nos permitan mejorar nuestro trabajo desde el punto de vista de "Gobierno de la Seguridad".

La nueva interfaz gráfica de Wireshark, como podemos ver en la imagen siguiente, presenta un diseño más de iconos que la anterior y es más amigable. Cuando nos preparamos para lanzar una captura, se nos despliega también una ventana con formato nuevo, que también nos parece más eficiente; inmediatamente nos informa sobre la interfaz que está recibiendo tráfico (*podemos ver en este caso que se trata de la WiFi: en1*), también en este formato tipo "tabla" de filas y columnas, podemos seleccionar cada opción (*como si fuera una celda*) y configurar cualquiera de ellas, en el ejemplo de esta imagen podemos ver que seleccionamos "Capture filter" y desplegamos una serie de opciones (*que están en memoria por haberlas empleado con anterioridad*) y desde allí es donde podemos seleccionar el filtro a aplicar (*recordemos que este formato de filtro de "captura" es del tipo **BPF**: Berkeley Packet Filter, dicho en otras palabras: formato "**tcpdump**"*).

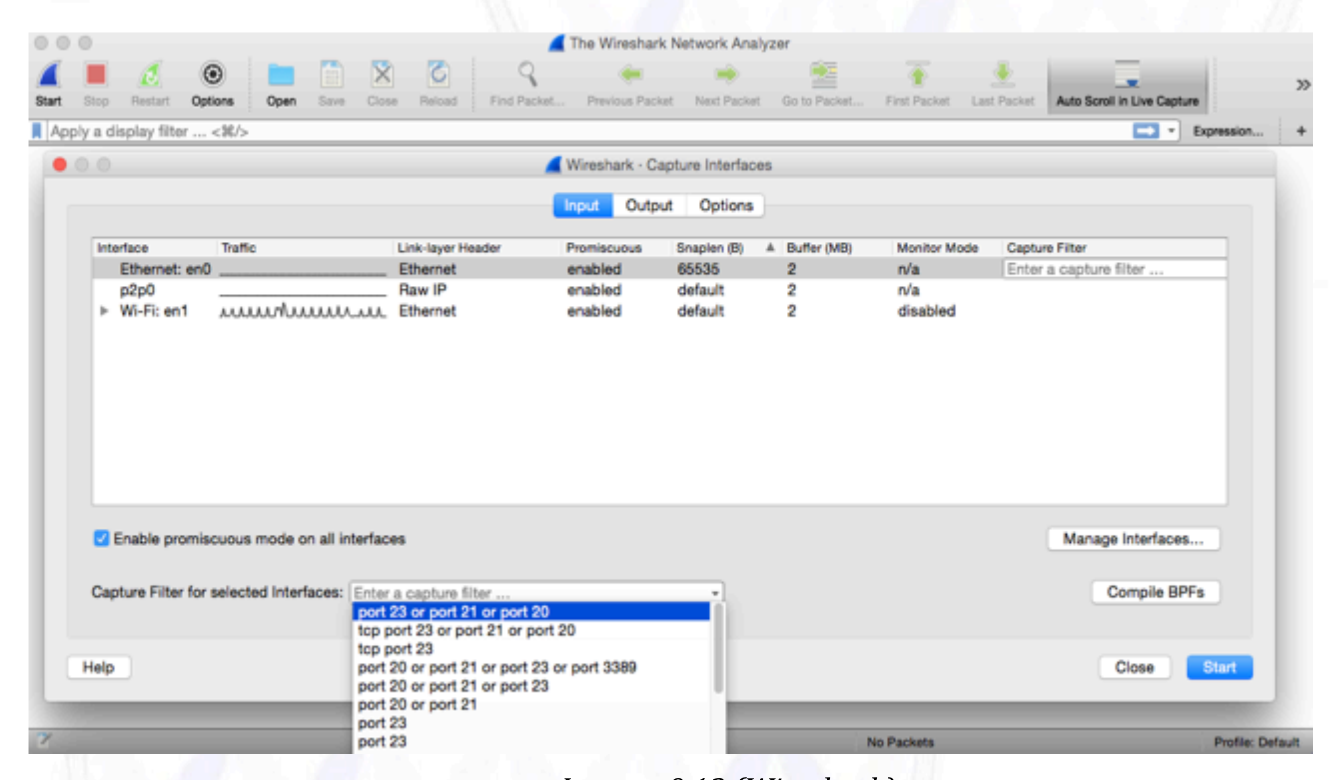


Imagen 9.13 (Wireshark)

Algo nuevo que también nos ofrece esta versión, es la ventana de "**Output**", en la cual podemos ver que es posible definir filtros permanentes, pero lo que a nuestro juicio es fundamental es la opción que figura abajo de poder "**Crear nuevos archivos automáticamente**", cada "x kilobytes" o "x segundos". Esta opción cuando dejamos sondas capturando sobre redes de alto tráfico, o sobre las que deseamos evaluar rangos horarios, es de suma importancia y la verdad, es que nos ha simplificado mucho el trabajo, es cierto que esto se pudo hacer toda la vida con el comando "**tcpdump**", o con scripts y el "**cron**" de

Linux pero ahora, como mencionamos al principio, lo hacemos de forma mucho más amigable.

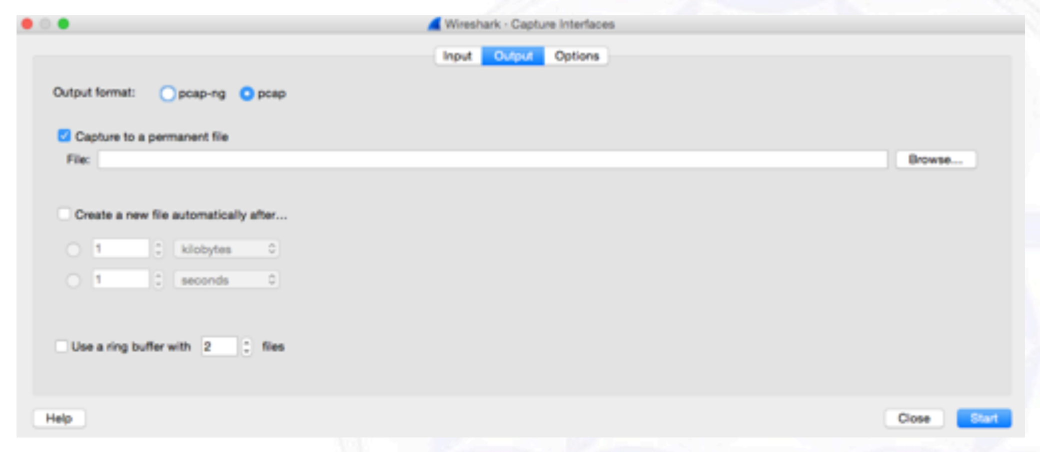


Imagen 9.14 (Wireshark)

Una vez ejecutadas las capturas, podemos aplicar los “filtros de visualización, en la imagen siguiente, por ejemplo, hemos seleccionado únicamente el puerto tcp.443 (TLS).

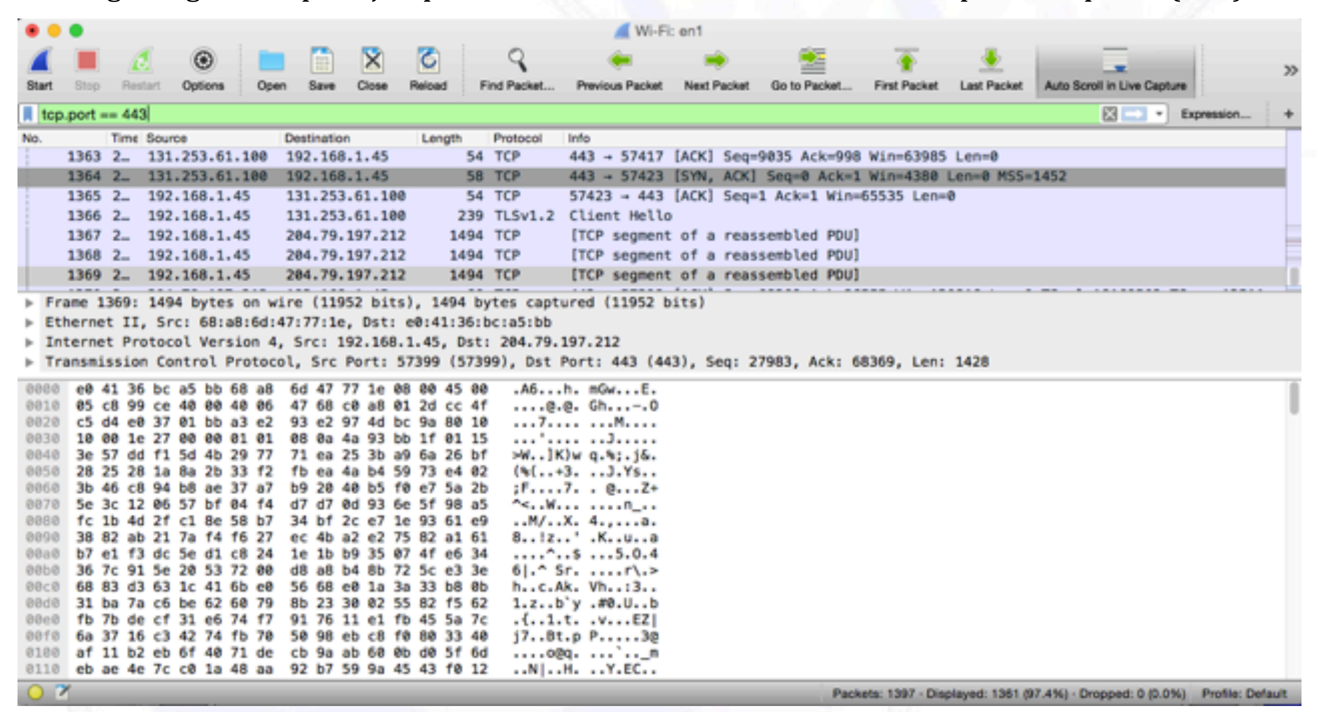


Imagen 9.15 (Wireshark)

Otro aspecto que ha cambiado para bien es la opción de “búsqueda”, que nos despliega un menú, sobre el cual podemos seleccionar diferentes opciones y dentro de cuál de las tres ventanas se ejecutará, en nuestro ejemplo hemos buscado la cadena (string) “google” en la ventana inferior (packet Byte), tened en cuenta que podemos buscar todo lo que haya viajado en esa captura (*nombres, password, mensajes, teléfonos, contenidos, direcciones, cuentas, etc.*).

Presentamos a continuación dos imágenes de este ejemplo.

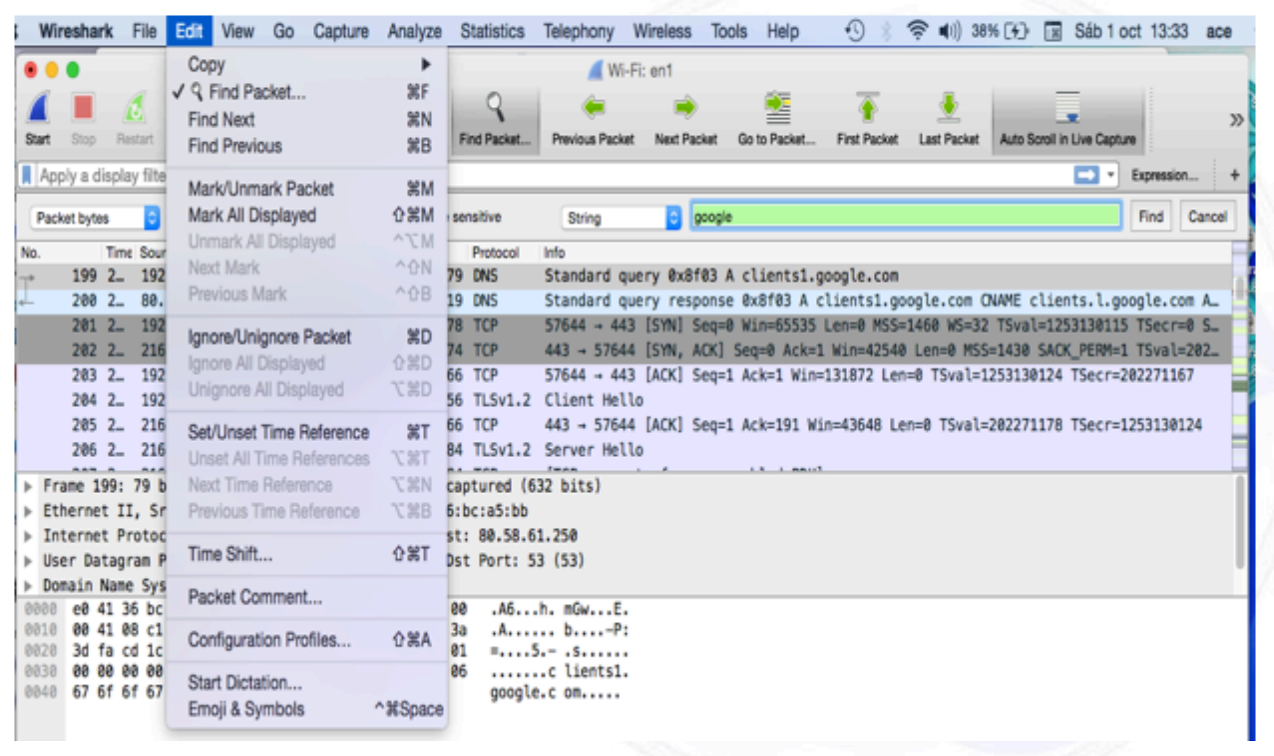


Imagen 9.16 (Wireshark)

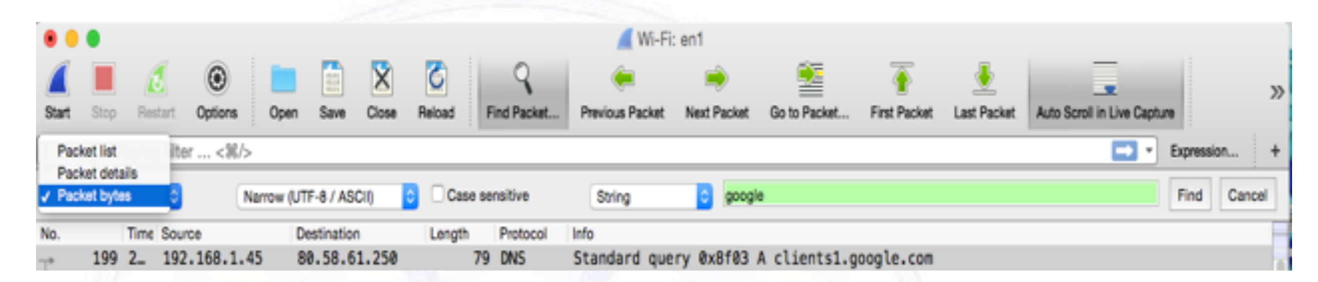


Imagen 9.17 (Wireshark)

Una opción que solemos emplear con mucha frecuencia es la de seguir flujos de tráfico para analizarlos con detalle:

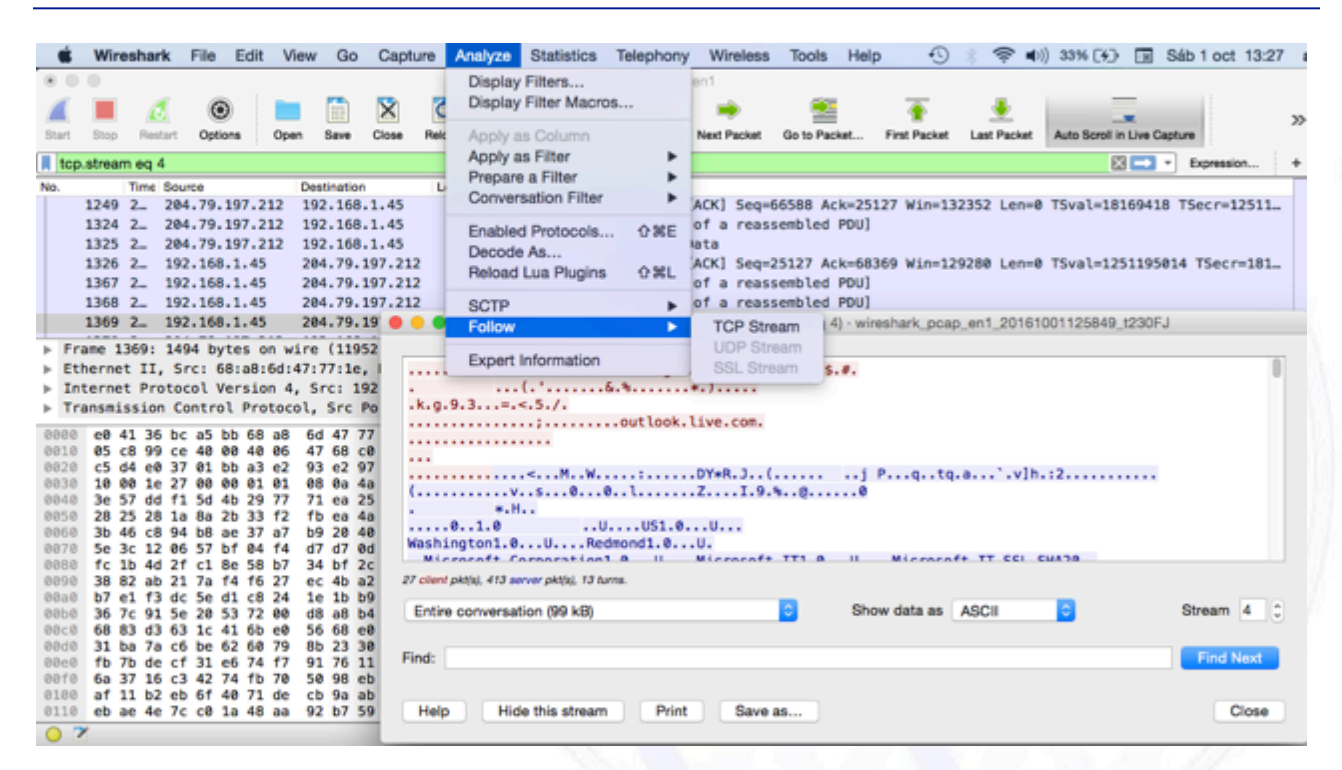


Imagen 9.18 (Wireshark)

Otra opción que nos ha resultado de mucha utilidad, en particular sobre capturas de VoIP o análisis de protocolo SIP es la de "**Gráficos de Flujo**", como podemos ver a continuación, nos resume todo el flujo de señalización de esta conversación.

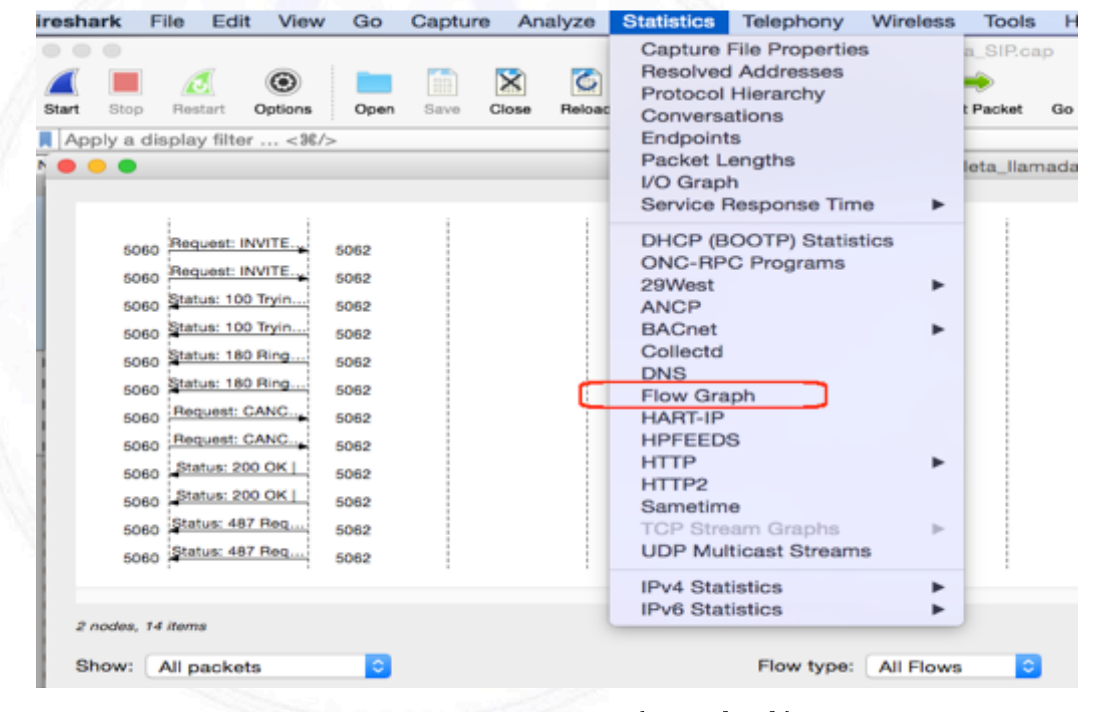


Imagen 9.19 (Wireshark)

Nuevamente, como hemos hecho a lo largo de todo este texto, invitamos al lector a que continúe profundizando sobre el empleo casi "ilimitado" que nos ofrece esta herramienta, no es nuestro objetivo dar cursos sobre el uso de la misma, sino sencillamente presentarla en virtud de la importancia que tiene para nuestro trabajo, poner algunos ejemplos prácticos de la misma y sobre todo, despertar el interés del lector sobre todo lo que puede ofrecerle el conocimiento y empleo de ell para la seguridad de sus redes.

9.6. Sistema Syslog.

Un Log (o registro) es de un tipo u otro dependiendo de la aplicación de la que provenga (*facilities*) y del nivel de "gravedad" del evento que ha logueado (*priorities*).

Las facilities son:

- auth y authpriv: para autenticación.
- cron: proviene servicios de programación de tareas, cron y atd.
- daemon: afecta un demonio sin clasificación especial (DNS, NTP, etc.).
- ftp: el servidor FTP.
- kern: mensaje que proviene del núcleo.
- lpr: proviene del subsistema de impresión.
- mail: proviene del subsistema de correo electrónico.
- news: mensaje del subsistema Usenet (especialmente de un servidor NNTP — protocolo de transferencia de noticias en red, «Network News Transfer Protocol» — que administra grupos de noticias).
- syslog: mensajes del servidor syslogd en sí.
- user: mensajes de usuario (genéricos).
- uucp: mensajes del servidor UUCP (programa de copia Unix a Unix, «Unix to Unix Copy Program», un protocolo antiguo utilizado para distribuir correo electrónico).
- local0 a local7: reservados para uso local.

las priorities son:

- emerg: Hay una emergencia y el sistema probablemente está inutilizado.
- alerta: Tener cuidado, cualquier demora puede ser peligrosa, hay que actuar.
- crit: las condiciones son críticas.

- err: error.
- warn: advertencia (error potencial).
- notice: las condiciones son normales pero el mensaje es importante.
- info: mensaje informativo.
- debug: mensaje de depuración.

Sintaxis del selector

El selector es una lista separada por punto y coma de pares **subsistema.prioridad** (*por ejemplo: auth.notice;mail.info*).

Un **asterisco** puede representar todos los subsistemas o todas las prioridades (*por ejemplo: *.alert o mail.**). Puede agrupar varios subsistemas separándolos con una coma (*por ejemplo: auth,mail.info*). La prioridad indicada también incluye los mensajes de prioridad igual o mayor; por lo tanto, auth.alert indica los mensajes del subsistema auth de prioridad alert o emerg. Si se agrega un signo de exclamación **"!"** como prefijo, indica lo contrario; en otras palabras, prioridades estrictamente menores. Por lo tanto, auth.!notice sólo incluye los mensajes del subsistema auth con prioridades info o debug. Si se agrega un signo igual **"="** como prefijo corresponde única y exactamente con la prioridad indicada (*Ejemplo: auth.=notice sólo incluye los mensajes del subsistema auth con prioridad notice*).

Cada elemento en la lista del selector reemplaza elementos anteriores. Así es posible restringir un conjunto o excluir ciertos elementos del mismo. Por ejemplo, kern.info;kern.!err significa los mensajes del núcleo con prioridades entre info y warn. La prioridad none indica el conjunto vacío (ninguna prioridad) y puede servir para excluir un subsistema de un conjunto de mensajes. Por lo tanto *.crit;kern.none indica todos los mensajes con prioridad igual o mayor a crit que no provengan del núcleo.

Los logs generalmente se guardan en archivos ubicados en el directorio **/var/log**, aunque muchos programas manejan sus propios logs y los guardan en /var/log/<programa>. Además, es posible especificar múltiples destinos para un mismo mensaje. Algunos de los log más importantes son:

- **/var/log/messages**: aquí encontraremos los logs que llegan con prioridad info (información), notice (notificación) o warn (aviso).
- **/var/log/kern.log**: aquí se almacenan los logs del kernel, generados por klogd.
- **/var/log/auth.log**: en este log se registran los login en el sistema, las veces que hacemos su, etc. Los intentos fallidos se registran en líneas con información del tipo invalid password o authentication failure.

- **/var/log/dmesg**: en este archivo se almacena la información que genera el kernel durante el arranque del sistema. Podemos ver su contenido con el comando dmesg: $dmesg

Los archivos de log crecen y con el tiempo se pueden volver muy extensos, pero no tenemos que preocuparnos porque en **/etc/cron.daily** (tareas que se ejecutan cada día) está el script **/etc/cron.daily/logrotate**, (cuyo archivo de configuración es **/etc/logrotate.conf**), que se encarga de comprimirlos y aplicar una rotación de archivos, añadiéndoles la extensión **.1.gz, .2.gz, etc**., volviendo a crear uno vacío (cuanto mayor sea el número más antiguo será el log).

Se debe tener en cuenta que no siempre el destino tiene que ser un fichero, otra posibilidad es mandar el log a:

- un usuario, basta con poner el nombre del usuario (por ej: root)
- a todos lo usuarios, poniendo * (asterisco)
- a otro programa, a través de un pipe, por ejemplo: |/nombre_del_prog
- a otro host, por ejemplo: @host.dominio
- a un terminal, como en el ejemplo visto antes.

Veamos un ejemplo:

```
-------------------------------------------------------------------
auth.crit @logger.ejemplo.com
auth.crit |/root/detector
auth.crit root
-------------------------------------------------------------------
```

syslogd manda todos los mensajes de autenticación con prioridad crítica a otra máquina (logger.ejemplo.com), a un programa que se llama detector y por último al root.

Cuando un programa envía un log a syslogd utiliza la función syslog() que está definida en syslog.h que se encuentra generalmente en /usr/include.

El primer parámetro de syslog es el nivel de prioridad, seguido del mensaje.

Las prioridades posibles vienen definidas en syslog.h, y son:

```
#define LOG_EMERG 0 /* system is unusable */
#define LOG_ALERT 1 /* action must be taken immediately */
#define LOG_CRIT 2 /* critical conditions */
#define LOG_ERR 3 /* error conditions */
#define LOG_WARNING 4 /* warning conditions */
#define LOG_NOTICE 5 /* normal but significant condition */
#define LOG_INFO 6 /* informational */
#define LOG_DEBUG 7 /* debug-level messages */
```

Uno de los problemas que tiene que afrontar un administrador cuando configura su sistema es dónde poner los ficheros de log, esta decisión es mu importante porque en caso de intrusión son la única prueba que se tiene. Si los ficheros de Log están en la misma máquina, el intruso solo tiene que modificar el fichero con un editor normal.

Syslogd central

Si se envían Logs a otro host, en el servidor syslogd (*históricamente*) había que revisar dos cosas. La primera que esté configurado para aceptar conexiones remotas. Para ello hay que añadir el parámetro **"-r"** a la línea de arranque. Ya sea en el script de **/etc/init.d/syslog**, o si lo arrancamos a mano. En el script de **init.d** suele ser en la variable donde se especifican los parámetros:

```
SYSLOGD_OPTIONS="-r -m 0"
```

Y si lo arrancáramos a mano:

```
# syslogd -r -m 0
```

En el caso de Debian (o en nuestro caso con Kali), en el directorio **/etc** podemos ver el archivo "**syslog.conf**", dentro del mismo en la actualidad, como podemos ver a continuación, tenemos comentadas **(#)** las líneas para que abra (deje en escucha) los puertos UDP o TCP para la recepción remota de Logs

```
# provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
```

Si analizamos el estado actual de los puertos locales de nuestro Kali veremos lo siguiente:

```
root@kali:/var/log# nmap localhost
     Nmap scan report for localhost (127.0.0.1)
     PORT   STATE SERVICE
     22/tcp open  ssh
```

Si por ejemplo, quitamos los comentarios de las 3 líneas de TCP y reiniciamos el rsyslog con el siguiente comando

```
# /etc./init.d rsyslog restart
```

Y nuevamente ejecutamos nmap, veremos que ahora está en escucha el puerto TCP 514 (syslog) y por lo tanto si desde otro host, le configuramos el sistema de Logs para que los envíe aquí, nuestro Kali se convertiría en un repositorio de Logs.

```
root@kali:/var/log# nmap localhost
```

```
PORT    STATE SERVICE
22/tcp  open  ssh
514/tcp open  shell     Puerto TCP 514 abierto
```

En resumen, actualmente con esta nueva estrategia de rsyslog, con el agregado de estas dos líneas es posible habilitar y/o deshabilitar la recepción de syslog por TCP o UDP con sólo comentar o descomentarlas.

Clientes syslogd

A la hora de configurar los clientes que van a enviar los logs al servidor central, únicamente tenemos que especificar qué logs van a ir al servidor central, lo haremos nuevamente en el fichero de configuración **/etc/syslog.conf**.

Una línea estandar es esta por ejemplo, en la que mandamos a **/var/log/messages** los logs de cron, info, mail, etc:

```
*.info;mail.none;authpriv.none;cron.none          /var/log/messages
```

Para que estos logs se dejen de almacenar en el Log local y pasen al remoto, únicamente indicamos con **@servidor_syslogd** el **hostname/ip del servidor syslogd**. Si por ejemplo, el servidor syslogd tiene el hostname syslogd01, la misma línea anterior quedaría:

```
*.info;mail.none;authpriv.none;cron.none         @syslogd01
```

Ejercicio: si quisiéramos que nuestro Kali cuando se cambian los privilegios de usuarios, como al ejecutar un su envíe logs a nuestra máquina de salto, deberíamos incluir en su **/etc/syslog.conf**.

```
authpriv.* @10.0.0.100
```

Reiniciamos syslogd y comenzaríamos a enviar los logs al servidor central:

```
# /etc./init.d/./rsyslog restart
```

Un ejemplo de como veríamos el Log central con varias entradas de distintos servidores (servidor01, servidor02,...):

```
Aug 12 18:15:58 servidor01 snmpd[27557]: Connection from UDP: [xx.xx.xx.xx]:39892
Aug 12 18:15:58 servidor01 snmpd[27557]: Received SNMP packet(s) from UDP: [xx.xx.xx.xx]:39892
Aug 12 18:15:58 servidor02 snmpd[27557]: Connection from UDP: [xx.xx.xx.xx]:56751
```

```
Aug 12 18:15:58 servidor02 snmpd[27557]: Received SNMP packet(s) from UDP:
[xx.xx.xx.xx]:56751
…………………
……….
.
```

9.7. "John the Ripper" y "mutator".



Desde el punto de vista del "Gobierno de la Seguridad", en muchos casos es importante evaluar el nivel de Seguridad o robustez de las contraseñas que se están empleando en nuestras redes, aunque en nuestros procedimientos de "Autenticación y Control de Accesos" hayamos especificado con todo el detalle el formato mínimo y los períodos a los que deben responder, la realidad en muchos casos difiere la realidad de lo escrito.

Cuando estuvimos tratando "**Routing**" ya pusimos de manifiesto este hecho, e hicimos hincapié en las "password 7" de Cisco. En esta sección, a través de la herramienta "**John the Ripper**" desarrollaremos también cómo puede emplearse la misma para verificar si otro tipo de password han sido configuradas cumpliendo la normativa establecida o no.

Es importante que periódicamente se realice este tipo de evaluaciones, y seguramente será de máxima utilidad para demostrar el grado de cumplimiento de lo escrito. La mejor evidencia para cualquier responsable de dispositivos es presentarle la realidad pura y dura, por lo tanto si en un informe o reporte, se le describe el listado de usuarios que no cumplen con lo establecido, esto constituye una prueba contundente e irrefutable para que se tomen las acciones correspondientes y se logre mejorar el nivel de seguridad de nuestra red.

En el mercado existen varias herramientas de "Crackeo" de contraseñas, pero nos hemos centrado en "John the Ripper" pues (*al igual que el autor….),* es una de las más antiguas del mercado y reconocida en todos los ámbitos por su eficiencia, en su página oficial (http://www.openwall.com/john/)la describe como la "**más rápida del mercado**" y es posible que lo sea. Para nosotros es sólo una presentación de la misma, con la que deseamos despertar el interés del lector en el empleo de este tipo de software, pero por supuesto queda en la libre decisión de cada uno el empleo de la que más le guste.

Dentro del sistema operativo "Kali" ya está instalado. Si abrimos una consola y ejecutamos el comando "**john**", nos presentará lo siguiente:

```
root@kali:~# john
    John the Ripper password cracker, version 1.7.8
    Copyright (c) 1996-2011 by Solar Designer
    Homepage: http://www.openwall.com/john/

    Usage: john [OPTIONS] [PASSWORD-FILES]
```

```
--single                    "single crack" mode
--wordlist=FILE --stdin     wordlist mode, read words from FILE or stdin
--rules                     enable word mangling rules for wordlist mode
--incremental[=MODE]        "incremental" mode [using section MODE]
--external=MODE             external mode or word filter
--stdout[=LENGTH]           just output candidate passwords [cut at LENGTH]
--restore[=NAME]            restore an interrupted session [called NAME]
--session=NAME              give a new session the NAME
--status[=NAME]             print status of a session [called NAME]
--make-charset=FILE         make a charset, FILE will be overwritten
--show                      show cracked passwords
--test[=TIME]               run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]   [do not] load this (these) user(s) only
--groups=[-]GID[,..]        load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]      load users with[out] this (these) shell(s) only
--salts=[-]COUNT            load salts with[out] at least COUNT passwords only
--format=NAME               force hash type NAME: DES/BSDI/MD5/BF/AFS/LM/crypt
--save-memory=LEVEL         enable memory saving, at LEVEL 1..3
```

Estos párrafos no serán una guía de empleo de John the Ripper, sino sencillamente una descripción de sus funciones básicas, con la intención que el lector pueda conocerlo, comenzar a emplearlo y luego si es de su interés, puede encontrar en Internet miles de artículos sobre el mismo.

Lo más importante desde el punto de vista “criptográfico” del mismo, es que fundamentalmente este software nos ofrece dos alternativas:

a) Fuerza bruta.

b) Ataque de diccionario.

El concepto de “Fuerza bruta” es muy claro, irá lanzando combinaciones, incrementando la cantidad de caracteres dentro del rango que definamos, y a cada combinación le aplicará el algoritmo buscado, si el resultado de esta operación es idéntico a la contraseña buscada, entonces es un “acierto” y esa combinación en concreto es la palabra “clave” original. Estas combinaciones pueden ser de solo texto (ASCII), de texto y números, de lo anterior, más caracteres especiales y considerando o no con mayúsculas y minúsculas. Todo esto es parametrizable, pero lo que debemos considerar como base de esta operación es que, cuando la contraseña comienza a adoptar medidas robustas (*longitud, combinación de caracteres con números y especiales, etc…*), este ataque de fuerza bruta puede llegar a ser eterno… y básicamente esto es lo que debemos fomentar desde el área de Seguridad….

Que para descifrar nuestras contraseñas, sencillamente: no se justifique el esfuerzo por parte de un intruso.

Prestad mucha atención al párrafo anterior: No estamos diciendo que sean “**irrompibles**” pues si somos conscientes del inimaginable avance de la potencia informática, lo que hoy es imposible, mañana lo será (*y así lo demuestra toda la historia de la criptografía*). Hay que tener mucho cuidado con esto, pues no debemos saturar a los administradores o usuarios de red con una política de contraseñas inabordablemente

pesada……. Pues caerá en el olvido, el incumplimiento o la rutina seguramente. Nuestro compromiso (y no es fácil) es lograr identificar las plataformas, segmentos o dispositivos críticos, ser más exigentes con estos, luego una segunda línea de criticidad, menos exigente, y finalmente un tercer nivel que puede ser más "Light" pues el impacto para la organización es mínimo. Este "**grado de compromiso**" entre no pasarnos de exagerados (*y que no se cumpla*) o ser demasiado "permisivos" (*y debilitar todo*), **no es nada fácil**. Requiere, de verdad ,un trabajo progresivo y constante de ajuste y concientización a lo largo del tiempo.

Volvamos a las alternativas de ataques, la segunda que nos ofrece "John the Ripper" es el ataque de diccionario. Esta técnica en principio se trata de tomar "palabras" establecidas en un fichero de texto que denominaremos "diccionario" y aplicarle el algoritmo de cifrado correspondiente, si el resultado coincide con la password buscada acertará, caso contrario el programa recorrerá todo el fichero de texto, procesando cada una de las palabras y finalizará indicándonos que no tuvo éxito. Como podemos deducir aquí el aspecto clave es el diccionario que vayamos a emplear, pero no sólo por su longitud o tamaño, sino por sus "características". Existen cientos de diccionarios que podemos descargar de Internet, y recomendamos que sean empleados, pero en nuestro caso en particular trabajando sobre nuestras propias redes tenemos una gran ventaja, pues lo que estamos haciendo en realidad se denomina: "**Auditoría de Seguridad de Hacking ético con técnicas de caja blanca**", es decir que contamos con toda la información que necesitemos: nombres de cuentas de usuarios, acceso a plataformas y servidores, ficheros de configuración, etc. Nuestra experiencia es que es mucho más eficiente, realizar un trabajo previo de análisis de esta información, recolectar todo dato que nos sea de utilidad y crear inicialmente nuestro fichero de "usuarios". En primer lugar, no es de extrañar que aplicando sólo este, nos encontremos la sorpresa que emplean este nombre también como password (root:root, admin:admin, cisco:cisco, jlopez:jlopez, sr34021:sr34021…. *Aunque a esta altura del siglo parezca increíble…… la realidad no deja de sorprendernos*). En segundo lugar, existen técnicas de John y también software adicional que nos permiten generar ficheros de "diccionario_password" basado en este listado de usuarios realizando permutaciones, combinaciones, etc… Este tipo de diccionarios son los que mayor factor de éxito nos ha dado en este trabajo.

Si deseamos emplear este tipo de diccionarios el comando para ello es:

```
root@kali:~# john --wordlist=nombre_diccionario  fichero_password
```

En unos párrafos más abajo veremos cómo podemos "personalizar" nuestros diccionarios .

El modo más sencillo para ejecutar John the Ripper es: con la opción "--single". El cual comienza con pasos básicos y a medida que no logra encontrar la password va incrementando el nivel. Siempre podremos "personalizar" también casi todos los parámetros de John, en el caso de las reglas utilizadas en este modo, por ejemplo podemos acceder a ellas en el la sección "**List.Rules:Single"** del archivo de configuración "john.conf , que en "kali" está en /etc/john/john.conf, prácticamente en las primeras líneas. Presentamos el principio de esa sección a continuación:

```
root@kali:~# vi /etc/john/john.conf
    …….
    …
```

```
.
# "Single crack" mode rules
[List.Rules:Single]
# Simple rules come first...
:
-s x**
-c (?a c Q…………
….
..
```

A continuación presentamos el formato que tendría esta opción "--single":

```
root@kali:~# john --single fichero_password
```

John the Ripper permite también utilizar el modo "**Incremental**", que prácticamente usa todas las combinaciones posibles de un cierto conjunto de caracteres.

Se puede optar también por utilizar opciones alfabéticas "Alpha" o "Digits" si sólo preferimos que use números. A continuación presentamos ejemplos del mismo.

```
root@kali:~#  john --incremental fichero_password
```

O también como sigue a continuación:

```
root@kali:~# john -i fichero_password
```

Si sólo queremos que sólo pruebe con números:

```
root@kali:~# john -i:Digits fichero_password
```

Si sólo queremos que sólo pruebe con letras:

```
root@kali:~# john -i:Alpha fichero_password
```

Pero de todo lo mencionado, lo que a nosotros nos ha dado mayor resultado, como hemos mencionado con anterioridad, es aprovechar el conocimiento que tenemos de nuestras redes y realizar previamente una buena recolección de nombres y en lo posible también contraseñas.

Por ejemplo, volvamos a nuestra configuración de ese curso que tratamos en la sección de túneles SSH, aprovechemos los usuarios "**curso**" y **"curso1**" a los cuáles les hemos configurado dos passwords triviales y presentaremos a continuación:

Ejemplo:

Consultamos el fichero **/etc/password** y vemos lo siguiente:

```
curso:x:1000:1000:curso,,,:/home/curso:/bin/bash
curso1:x:1005:1005:,,,:/home/curso1:/bin/bash
```

Consultamos el fichero /etc/shadow y vemos lo siguiente:

```
curso:$6$NRTfYmBP$nF6IhyIT2sKRQDB8S5Z0SVREv8H4qu8jCEhHBMT2bSp//iESgj8d1ZiKyDwr0.drdw9qHOxFmDjkV4qzZl84P0:17072:0:99999:7:::
curso1:$6$hz0/HrOM$dQSkA20dlsJTLkSHCgJ9ULD9eyl.AgJ/Xzn0/./XsMo1AfVwPPa/3mWrkXrLgblB.LWjIHYiv7A5vvV7cPiBS/:17072:0:99999:7:::
```

Si ejecutamos en modo básico "John the Ripper" vemos que:

```
root@kali:~#  john prueba
    Loaded 2 password hashes with 2 different salts (generic crypt(3) [?/32])
    curso           (curso)
    guesses: 1  time: 0:00:00:13 43% (1)  c/s: 80.30  trying: /curso199999 - mrCurso1
    12345678        (curso1)
    guesses: 2  time: 0:00:00:37 100% (2)  c/s: 77.16  trying: 12345 - missy
    Use the "--show" option to display all of the cracked passwords reliably
```

Hemos destacado en rojo, las contraseñas de cada usuario y la velocidad con la que las resolvió.

Para consultar las contraseñas que ya ha roto, podemos hacerlo como se presenta a continuación (*es importante tener en cuenta que si repetimos nuevamente la ejecución sobre este mismo fichero pero con más contraseñas, estas ya nos las procesará, solo verificará que sigan iguales*):

```
root@kali:~# john --show prueba
    curso:curso:17072:0:99999:7:::
    curso1:12345678:17072:0:99999:7:::

    2 password hashes cracked, 0 left
```

Con los breves conceptos sobre "John the Ripper" ya podemos comenzar a trabajar, y por supuesto profundizar todo lo que deseemos, pues tal como dijimos es un software que lleva muchos años de rodaje y nos ofrece muchísimas más opciones para seguir profundizando, así que ya es momento de "hincar los codos" como se dice en España y comenzar a estudiarlo en detalle.

Para cerrar este tema, sólo nos queda presentar un muy buen método para construir diccionarios robustos, sobre los que insistimos, desde el punto de vista de la Seguridad contamos (*o deberíamos contar*) con alto grado de información de nuestras redes, y por esta razón la construcción de estos "diccionarios personalizados" es el método más eficiente para velar por el uso de nuestras contraseñas. Tal vez sea diferente la situación de un intruso pues él se supone que tiene menos información que nosotros (*o al menos eso sería de esperar.........*) y tal vez esta persona prefiera emplear otras técnicas, pero no es nuestro caso.

Para este trabajo, proponemos el empleo del software "mutator" que es una herramienta escrita en "c" y también es Open Source. Este no viene instalado en "Kali", por lo tanto tendremos que instalarlo.

Esta herramienta nos permitirá realizar:

- Mutaciones de mayúsculas/minúsculas
- Añadir caracteres especiales
- Anexar cadenas de una lista previamente definida
- Añadir diferentes formatos de fecha

Podemos descargar los paquetes para Kali en (*recomendamos descargar la última versión*):

https://bitbucket.org/alone/mutator/downloads

Una vez descargados, su instalación es verdaderamente sencilla:

```
root@kali:~# #tar -xvzf mutator_release-v0.2.2-1-gc29ce2b.tar.gz
             mutator/
             mutator/.gitignore
             mutator/COPYING
             mutator/INSTALL
             mutator/Makefile
             mutator/README
             mutator/TODO
             mutator/main.c
             mutator/main.h
             mutator/misc.c
             mutator/misc.h
             mutator/mutator.c
             mutator/mutator.h
             mutator/test.txt
             mutator/types.h
root@kali:~# cd mutator/
root@kali:~# make
    gcc -I. -O3 -Wall -Wextra -g -pedantic -std=c11 -c misc.c
    gcc -I. -O3 -Wall -Wextra -g -pedantic -std=c11 -c main.c
    gcc -I. -O3 -Wall -Wextra -g -pedantic -std=c11 -c mutator.c
```

Una vez instalado se ejecuta con la siguiente opción:

```
root@kali:~#./mutator
  Mutator v0.2 by @AloneInTheShell email:<alone.in.the.shell@gmail.com>
  Syntax: mutator [options] wordlist

    Options:
       -v, --version          Show version information
       -h, --help             Show this help
       -o, --output [file]    File to write the results
       -f, --file [file]*     File from read the words
       -w, --word [word]*     Word to mutate
       -b, --basic            Only "case" and "l33t" mutations
       -a, --advanced         Only advanced mutations
```

```
-y, --years=[year]     No append,prepend year, if a
year is specified appendrange between year specified
and actual year, you can specified a range as well
[year-year]
-x, --specials    No append specials chars
-s, --strings     No append,prepend hardcoded strings

One of these options -w or -f is required
```

Esta herramienta tiene un módulo llamado "**mutator.c**" que contiene una sección que es desde donde se pueden definir los caracteres especiales que se deseen utilizar, también los caracteres que se decida reemplazar y las cadenas adicionales que hemos mencionado.

Como ejemplo, vamos a crear un fichero llamado "**nombres**" cuya única línea sea "**admin**". Luego ejecutaremos:

```
root@kali:~#./mutator -f nombres -o diccionario1.txt
[+] Number of words to mutate: 1
[+] Current word: 'admin'
    [-] Basics mutations generated: 6
    [-] To leet mutations generated: 5
    [-] Special chars mutations generated: 108
    [-] Append strings mutations generated: 1053
    [-] Append year mutations generated: 1170
[+] Total mutations generated: 1170

root@kali:~# ls -l | grep diccionario1.txt
-rw-r--r-- 1 root root 11259 Sep 28 16:44 diccionario1.txt

root@kali:~# vi diccionario1.txt
    admin
    ADMIN
    Admin
    admiN
    AdmiN
    4dm1n
    Adm1n
    4dm1N
    ……
    …  ← Siguen las mil líneas
    .
    4dm1n+1234
    Adm1n+1234
    4dm1N+1234
    Adm1N+1234  ← Fin
```

Como pudimos ver en el ejemplo, sin habernos puesto a generar listas, fechas o caracteres especiales, con la sencilla configuración básica, ya nos ha potenciado por mil, nuestro diccionario de búsqueda, el cual insistimos se basará en palabras que ya son claves dentro de nuestra organización y por lo tanto su índice de aciertos será aún mayor que

cualquier otro diccionario descargado de Internet, lo cual no quita que usemos ambos o que hagamos varios "mix" de todos ellos. Nuevamente, nuestra propuesta es que dediquéis todo el tiempo posible a seguir avanzando en el estudio de este tipo de herramientas.

9.8. medusa / hydra.

Podríamos discutir un buen rato acerca de las ventajas y desventajas de estas dos herramientas, también confrontarlas para comparar cuál es mejor. Por nuestra parte, no vamos a perder tiempo en ello, solamente presentar unas breves líneas sobre ambas y como están incluidas en "Kali", presentaremos algunos sencillos ejemplos de su uso para que el lector las conozca y luego pueda seguir adelante con un estudio detallado y seleccionar la que más le guste, o emplear ambas.

Estas herramientas nos ofrecen la posibilidad de evaluar la fortaleza de nuestra red frente a ataques de fuerza bruta o de diccionario a través de los protocolos: telnet, ftp, snmp, http, pop3, etc.

> **NOTA IMPORTANTE:** Estas herramientas las emplearemos generando altos volúmenes de tráfico en nuestras redes, por lo tanto, se deberá tener MUCHA CAUTELA en su uso, pues pueden ocasionar caídas de servicios o saturar dispositivos o segmentos de red.

Para aprovechar al máximo su potencia, primero debemos contar con buenos diccionarios, tanto de contraseñas como de usuarios, por esa razón es que en la sección anterior hemos presentado "**mutator**" como base de comprensión de este tipo de programas y desarrollos, también hicimos referencia a la "ventaja competitiva" que nos da el conocimiento de nuestra infraestructuras a la hora de generar este tipo de listados.

Con este punto ya comprendido, pasemos a presentar ahora "**hydra**" y "**medusa**".



La página Web de **medusa** es: http://www.foofus.net



La página Web de **hydra** es: https://www.thc.org/thc-hydra

Como ya hemos mencionado ambos programas ya están instalados en "Kali" por lo que solamente necesitamos abrir una consola y ejecutarlos. Para ir analizando sus opciones, presentamos a continuación, en primer lugar "medusa", ejecutando únicamente su nombre:

```
root@kali:~# medusa
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun/Foofus Networks <jmk@foofus.net>

      ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C
    file] -M module [OPT]
  -h [TEXT]: Target hostname or IP address
  -H [FILE]: File containing target hostnames or IP addresses
  -u [TEXT]: Username to test
  -U [FILE]: File containing usernames to test
  -p [TEXT]: Password to test
  -P [FILE]: File containing passwords to test
  -C [FILE]: File containing combo entries. See README for more information.
  -O [FILE]: File to append log information to
  -e [n/s/ns]: Additional password checks ([n] No Password, [s] Password =
    Username)
  -M [TEXT]: Name of the module to execute (without the .mod extension)
  -m [TEXT]: Parameter to pass to the module. This can be passed multiple times
    with a different parameter each time and they will all be sent to the module
    (i.e. -m Param1 -m Param2, etc.)
  -d       : Dump all known modules
  -n [NUM]: Use for non-default TCP port number
  -s       : Enable SSL
  -g [NUM]: Give up after trying to connect for NUM seconds (default 3)
  -r [NUM]: Sleep NUM seconds between retry attempts (default 3)
  -R [NUM]: Attempt NUM retries before giving up. The total number of attempts
    will be NUM + 1.
  -t [NUM]: Total number of logins to be tested concurrently
  -T [NUM]: Total number of hosts to be tested concurrently
  -L       : Parallelize logins using one username per thread. The default is to
    process the entire username before proceeding.
  -f       : Stop scanning host after first valid username/password found.
  -F       : Stop audit after first valid username/password found on any host.
  -b       : Suppress startup banner
  -q       : Display module's usage information
  -v [NUM]: Verbose level [0 - 6 (more)]
  -w [NUM]: Error debug level [0 - 10 (more)]
  -V       : Display version
  -Z [TEXT]: Resume scan based on map of previous scan
```

Veremos algunas de las opciones que más nos interesan por ahora (que operan de forma muy similar a "hydra").

`-h:` nombre o dirección IP de host que deseo atacar.

`-H:` es el nombre del fichero en el cual detallamos una lista de hosts .

`-u y -U:` Si es minúscula, se trata de un único nombre de usuario a probar, si es mayúscula, se refiere al nombre de un fichero que contendrá nuestra lista de usuarios (*en hydra funciona igual*).

`-p y -P:` Si es minúscula, se trata de una única contraseña a probar, si es mayúscula, se refiere al nombre de un fichero que contendrá nuestra lista de contraseñas, en

general es aquí donde nos conviene emplear nuestro diccionario de password (*en hydra funciona igual*).

`-F:` Detendrá la ejecución al encontrar el primer acierto (*Esto nos es de utilidad si con uno sólo para nosotros es suficiente para continuar otra actividad, pero cuando se trata de varios hosts, no es recomendable su empleo*).

`-O:` Nombre del fichero de salida donde nos guardará los aciertos.

`-e:` Esta es una opción interesante, pues independientemente de la contraseña o diccionario que pongamos con la opción "`-p y –P`", ofrece dos opciones más (o la combinación de ambas) `[n / s / ns]`. Si seleccionamos "`n`" probará primero el usuario sin contraseña, si ponemos "`s`" probará la contraseña con el mismo nombre que el usuario (es decir user=passwd), y si ponemos "`ns`" probará ambas.

`-T:` cantidad de host que atacará de forma concurrente.

`-M:` es muy importante pues aquí se define el módulo a utilizar. telnet, ftp, http, etc.

`-v:` modo verbose, nos ofrece más información podemos seleccionar diferentes niveles de 0 a 6, siendo el 6 el que más grado de detalle nos ofrecerá).

Esta última opción, es la que prepara la forma en que lanzará el ataque, no es lo mismo atacar el servicio telnet que por ejemplo, el servicio de http (*o cualquier otro*), por lo tanto debemos aclararle cómo deseamos que opere. Si queremos hacer una consulta de qué módulos tenemos instalados, se hace con la opción "`-d`", tal cual presentamos a continuación:

```
root@kali:~# medusa -d
  Medusa v2.0 [http://www.foofus.net]  JoMo-Kun/Foofus Networks <jmk@foofus.net>

    Available modules in "." :

    Available modules in "/usr/lib/medusa/modules" :
      + cvs.mod : Brute force module for CVS sessions : version 2.0
      + ftp.mod : Brute force module for FTP/FTPS sessions : version 2.0
      + http.mod : Brute force module for HTTP : version 2.0
      + imap.mod : Brute force module for IMAP sessions : version 2.0
      + mssql.mod : Brute force module for M$-SQL sessions : version 2.0
      + mysql.mod : Brute force module for MySQL sessions : version 2.0
      + ncp.mod : Brute force module for NCP sessions : version 2.0
      + nntp.mod : Brute force module for NNTP sessions : version 2.0
      + pcanywhere.mod : Brute force module for PcAnywhere sessions : version 2.0
      + pop3.mod : Brute force module for POP3 sessions : version 2.0
      + postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
      + rexec.mod : Brute force module for REXEC sessions : version 2.0
      + rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
      + rsh.mod : Brute force module for RSH sessions : version 2.0
      + smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions :
      version 2.0
      + smtp-vrfy.mod : Brute force module for enumerating accounts via SMTP VRFY :
      version 2.0
      + smtp.mod : Brute force module for SMTP Authentication with TLS : version 2.0
```

```
+ snmp.mod : Brute force module for SNMP Community Strings : version 2.0
+ ssh.mod : Brute force module for SSH v2 sessions : version 2.0
+ svn.mod : Brute force module for Subversion sessions : version 2.0
+ telnet.mod : Brute force module for telnet sessions : version 2.0
+ vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 2.0
+ vnc.mod : Brute force module for VNC sessions : version 2.0
+ web-form.mod : Brute force module for web forms : version 2.0
+ wrapper.mod : Generic Wrapper Module : version 2.0
```

Esta consulta que figura en el párrafo anterior, son todos los módulos que pueden operar actualmente con medusa. Veamos entonces cómo se lanza, por ejemplo para "telnet":

```
root@kali:~# medusa -H target_telnet_hosts.txt -U usuarios_telnet.txt -P
   passwords.txt -M telnet -T 10 -O salida_medusa_telnet_01.txt
```

Veamos otro ejemplo sobre protocolo "snmp":

```
root@kali:~# medusa -H taget_snmp_hosts.txt -u root -P communities.txt -M
   snmp -T 10 –O salida_medusa_snmp.txt
```

Continuemos esta sección con el software "**hydra**", que como hemos mencionado, opera de forma muy similar a medusa. Al igual que el anterior, si lo ejecutamos sin ninguna otra opción, nos ofrecerá la siguiente información:

```
root@kali:~# hydra

Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o
    FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x
    MIN:MAX:CHARSET]    [-SuvV46]    [server    service
    [OPT]]|[service://server[:PORT][/OPT]]

Options:
  -R        restore a previous aborted/crashed session
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get help
  -e nsr    try "n" null password, "s" login as pass and/or "r" reversed login
  -u        loop around users, not passwords (effective! implied with -x)
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to be attacked in parallel, one entry per line
  -o FILE   write found login/password pairs to FILE instead of stdout
  -f / -F   exit when a login/pass pair is found (-M: -f per host, -F global)
  -t TASKS  run TASKS number of connects in parallel (per host, default: 16)
  -w / -W TIME  waittime for responses (32s) / between connects per thread
  -4 / -6   prefer IPv4 (default) or IPv6 addresses
  -v / -V   verbose mode / show login+pass combination for each attempt
```

```
  -U       service module usage details
  server   the target server (use either this OR the -M option)
  service  the service to crack. Supported protocols: afp cisco cisco-enable cvs
    firebird ftp ftps http[s]-{head|get} http[s]-{get|post}-form http-proxy http-
    proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql
    mysql ncp nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres
    rdp rexec rlogin rsh sip smb smtp[s] smtp-enum snmp socks5 ssh svn teamspeak
    telnet[s] vmauthd vnc xmpp
  OPT      some service modules need special input (use -U to see module help)
Use HYDRA_PROXY_HTTP/HYDRA_PROXY and HYDRA_PROXY_AUTH environment for a proxy.

Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes.  Newest version available at http://www.thc.org/thc-hydra
The following services were not compiled in: sapr3 oracle.

Examples:
  hydra -l john -p doe 192.168.0.1 ftp
  hydra -L user.txt -p defaultpw -S 192.168.0.1 imap PLAIN
  hydra -l admin -P pass.txt http-proxy://192.168.0.1
  hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/DIGEST-MD5
```

Tal cual podemos ver y también presentamos anteriormente, su metodología de trabajo es muy similar a "**medusa**". No creemos necesario en este texto seguir con más detalles sobre esta herramienta, consideramos mucho más provechoso para el lector que comience a evaluar la misma personalmente, por medio de pruebas y búsquedas de ejemplos y guías de uso a través de Internet (*donde encontrará mucho al respecto*) y le será mucho más beneficioso.

9.9. nmap.

Esta herramienta la hemos presentado con bastante detalle en el libro "**Seguridad por Niveles**", por lo tanto no repetiremos estos conceptos, únicamente completaremos algunas opciones más que guardan relación con temas tratados en la presente obra.

Siempre yendo a las fuentes, recomendamos que para avanzar con más detalle sobre el empleo de esta herramienta, recurramos a:

https://nmap.org/man/es/man-port-scanning-techniques.html

Un puerto que no es recomendable dejar abierto es el puerto **79** "finger", pues como veremos a continuación nos ofrece inmediatamente la información de los usuarios conectados y también facilita otro tipo de ataques. Suele ser uno de los primeros escaneos que realizará un intruso, al menos para ir obteniendo listas de nombres. Desde nmap podemos analizarlo de forma masiva, a continuación se presenta el comando para analizar usuarios por medio de finger:

```
root@kali:~# nmap -n -p 79 -iL 172.20.0.0/16 -sC
```

También podemos emplear desde "**Kali**" el comando "**finger**", como presentamos a continuación:

```
root@kali:~# finger @10.20.111.3
Login       Name                TTY        Idle   When       Where
root        Super-User          console     12d Wed 16:52
oracle      Usuario Oracle Inter pts/1        7 Thu 16:09   10.75.25.239
root@kali:~#
```

Imagen 9.20 (ejecución del comando finger por consola)

Otra opción que solemos emplear y que es muy útil para armar listados desde rangos de direccionamiento IP y su máscara de red:

```
root@kali:~# nmap xxx.xxx.xxx.xxx/mask -sL
```

Ejemplo:

```
sh-3.2# nmap 192.168.1.0/24 -sL
    Starting Nmap 6.47 ( http://nmap.org ) at 2016-09-30 11:57 CEST
    Nmap scan report for 192.168.1.0
    Nmap scan report for 192.168.1.1
    Nmap scan report for 192.168.1.2
    ……
    ..
    .
    Nmap scan report for 192.168.1.255
```

La opción anterior suele ser útil para pasar estos rangos a listas, en general de herramientas que no controlan las opciones de máscara tipo "IP/mask" como nmap o para crear plantillas de informes, reportes, etc. (por supuesto que luego filtraremos "`Nmap scan report for`", y nos quedaremos solamente con las direcciones IP.

Otra opción, que ya hemos presentado en secciones anteriores es evaluar el protocolo **snmp** usando nmap (*como vemos en esta opción, estamos empleando "**-sU**" se trata de un escaneo solamente a protocolo UDP*):

```
sh-3.2# nmap –sU -p 161 IP/Red_destino –sV
```

Las opciones clásicas para escaneo de puertos, ya las hemos visto en el libro "Seguridad por Niveles", sólo reiteramos algunas pocas de las más "clásicas"de ellas:

Para verificar si host responde al ping (*la opción "**-n**" la ponemos para que no busque la resolución de nombres vía DNS*):

```
sh-3.2# nmap -n -sP 192.168.1.1
    Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-01 11:54 CEST
    Nmap scan report for 192.168.1.1
```

```
Host is up (0.0056s latency).
MAC Address: E0:41:36:BC:A5:BB (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Idem para todo un segmento de red:

```
sh-3.2# nmap -n -sP 192.168.1.0/24
    Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-01 11:58 CEST
    Nmap scan report for 192.168.1.1
    Host is up (0.0056s latency).
    MAC Address: E0:41:36:BC:A5:BB (Unknown)
    Nmap scan report for 192.168.1.33
    Host is up (0.0023s latency).
    MAC Address: F2:F2:6D:6D:A5:31 (Unknown)
    Nmap scan report for 192.168.1.35
    Host is up (0.054s latency).
    MAC Address: B0:89:91:F9:A9:86 (LGE)
    Nmap scan report for 192.168.1.39
    Host is up (0.074s latency).
    MAC Address: 30:19:66:37:52:FB (Samsung Electronics Co.)
    Nmap scan report for 192.168.1.44
    Host is up (0.025s latency).
    MAC Address: 44:87:FC:95:C0:97 (Elitegroup Computer System CO.)
    Nmap scan report for 192.168.1.48
    Host is up (0.074s latency).
    MAC Address: 00:23:4D:D3:99:D4 (Hon Hai Precision Ind. Co.)
    Nmap scan report for 192.168.1.45
    Host is up.
    Nmap done: 256 IP addresses (7 hosts up) scanned in 1.65 seconds
```

Una opción que nos suele ser de mucha utilidad a la hora de optimizar nuestro trabajo es "--exclude", si comparamos los párrafos que siguen a continuación con los que presentamos aquí arriba, se nota perfectamente su resultado:

```
sh-3.2# nmap -n  -sP 192.168.1.0/24 --exclude 192.168.1.40-50
    Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-01 12:42 CEST
    Nmap scan report for 192.168.1.1
    Host is up (0.0090s latency).
    MAC Address: E0:41:36:BC:A5:BB (Unknown)
    Nmap scan report for 192.168.1.33
    Host is up (0.0023s latency).
    MAC Address: F2:F2:6D:6D:A5:31 (Unknown)
    Nmap scan report for 192.168.1.34
    Host is up (0.072s latency).
    MAC Address: 00:03:AB:DF:4B:88 (Bridge Information Systems)
    Nmap scan report for 192.168.1.35
    Host is up (0.076s latency).
    MAC Address: B0:89:91:F9:A9:86 (LGE)
    Nmap scan report for 192.168.1.39
    Host is up (0.075s latency).
    MAC Address: 30:19:66:37:52:FB (Samsung Electronics Co.)
    Nmap done: 245 IP addresses (5 hosts up) scanned in 3.86 seconds
```

Para escanear puertos TCP (nmap posee un listado de unos 1000 puertos que son los más frecuentes, y prueba con esta lista,) , si deseamos más detalles (o nos interesa modificar este listado), en el caso de "Kali", tiene dentro del directorio "/usr/share/nmap" el fichero "nmap-services", en este, veremos los puertos con su respectiva descripción, nombre, etc. (y también otros ficheros que nos pueden ser de gran utilidad en este mismo directorio). Recomendamos profundizar sobre estos ficheros si el lector desea especializarse más en el empleo de esta herramienta:

```
sh-3.2# nmap -n -sT 192.168.1.1
     Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-01 11:54 CEST
     Nmap scan report for 192.168.1.1
     Host is up (0.017s latency).
     Not shown: 995 closed ports
     PORT    STATE    SERVICE
     21/tcp  filtered ftp
     22/tcp  open     ssh
     23/tcp  open     telnet
     80/tcp  open     http
     443/tcp open     https
     MAC Address: E0:41:36:BC:A5:BB (Unknown)
     Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

Si prestamos atención al comando anterior, nos muestra puertos "**filtered**" y "**open**" (*también en otros casos nos los muestra como "**close**"),* si sólo quisiéramos quedarnos con la información de los puertos "abiertos", una buena opción es "--open" como vemos a continuación:

```
sh-3.2# nmap -n -sT --open 192.168.1.1
      Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-01 12:31 CEST
      Nmap scan report for 192.168.1.1
      Host is up (0.016s latency).
      Not shown: 995 closed ports, 1 filtered port
      PORT    STATE SERVICE
      22/tcp  open  ssh
      23/tcp  open  telnet
      80/tcp  open  http
      443/tcp open  https
      MAC Address: E0:41:36:BC:A5:BB (Unknown)
      Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
```

Podemos apreciar en el comando anterior, que la línea "21/tcp filtered ftp" ya no aparece.

Si lo que deseamos es un poco más de detalles sobre ese host, podemos emplear la opción "-sV" que intentará resolver el sistema operativo destino:

```
sh-3.2# nmap -n -sV 192.168.1.44
     Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-01 12:29 CEST
     Nmap scan report for 192.168.1.44
     Host is up (0.010s latency).
```

```
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
111/tcp open  rpcbind 2-4 (RPC #100000)
MAC Address: 44:87:FC:95:C0:97 (Elitegroup Computer System CO.)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

